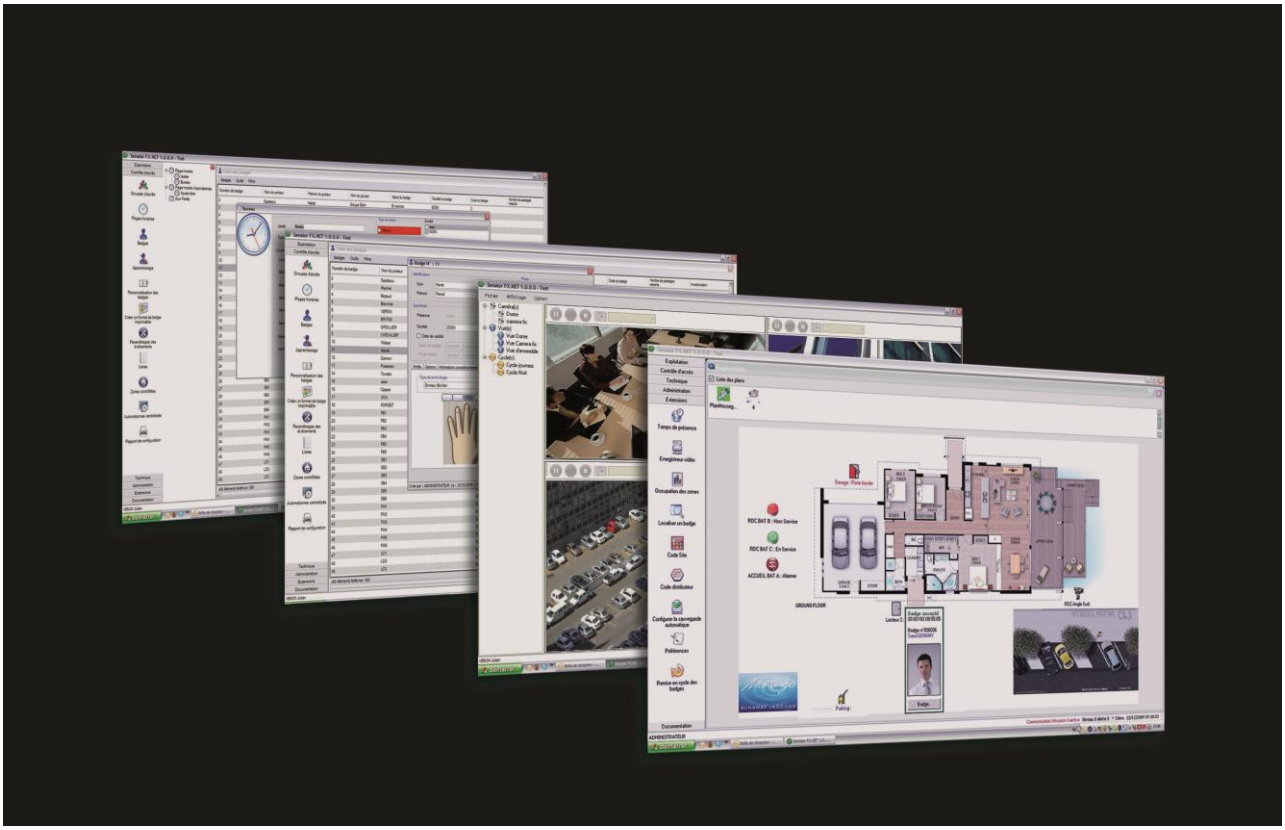
EDEN innovations

Contrôle d'accès

senator-fx.net / log.net

Manuel d'utilisation



Copyright © EDEN France LTD, 2010. Tous droits réservés. Le logiciel du système de contrôle d'accès intégré SENATORFX.NET® est protégé par la loi sur les droits d'auteur et traités internationaux.

Toute reproduction ou distribution de ce logiciel ou n'importe quelle partie de celui-ci, peut entrainer des peines civiles et criminelles sévères et des poursuites dommage pour le maximum permis par la loi.

Toutes autres marques de commerce et noms de produit sont des marques de commerce ou des marques de commerce déposées de leurs compagnies respectives.

Les informations contenues dans ce manuel de référence sont sujettes à changement sans préavis.

Remerciements

Cher(ère) client(e),

Vous venez de faire l'acquisition du logiciel de gestion d'accès

*« **SENATORFX.NET** ®» édité par la société française EDEN INNOVATIONS.*

Toute l'équipe EDEN INNOVATIONS vous remercie de votre intérêt ainsi que de votre confiance pour notre solution globale de sécurité.

Nous espérons qu'elle vous donnera entière satisfaction dans la sécurisation des locaux de votre entreprise.

Pour toutes remarques complémentaires, vous pouvez nous contacter via notre site Internet

www.eden-innovations.com

*L'équipe **EDEN INNOVATIONS**.*

Sommaire

« Installer et utiliser « SENATORFX.NET® » 8
Éditions de SENATORFX.NET® 9
Exigences du logiciel SENATORFX.NET® 10
Installation du logiciel SENATORFX.NET® 11
Installation du logiciel SENATORFX.NET® (suite) 12
Démarrer le logiciel SENATORFX.NET® 13
Applications multipostes clients-serveurs 14
Les modules complémentaires 15
Interface utilisateur de SENATORFX.NET 16
Survol de l'écran principal 17
Onglet et sous menus « Exploitation » 18
Onglet et sous menus « Contrôle d'accès » 19
Onglet et sous menus « Technique » 20
Onglet « Administration » et ses sous menus 20
Onglet et sous menus « Extensions » 21
Onglet et sous menus « Documentation » 22
Configuration du site 23
Création d'une installation 25
Gestion des bases de données 26
Le service Controller 27
Les réseaux de centrales 28
1.Ajouter un réseau 28
2.Création d'un réseau via liaison « Port Com » 29
3.Création d'un réseau via liaison « Port USB » 29
4.Création d'un réseau via liaison « Port Ethernet » 30
5.Modification/supression d'un réseau 31
6.Utilisation de la biométrie 32
Paramétrage des centrales 34
1.Création /modification d'une centrale 34
2.Dupliquer une centrale 38
3.Supprimer une centrale 39
Paramétrage des lecteurs 40
1.Configurer le type de lecteur 40
2.Détection automatique du format de badges existant 43
3.La biométrie 44
4.Paramétrer un lecteur 45

7.Onglet « Fonctions standards » 46
8.Onglet « Fonctions spéciales » 47
9.Onglet « Profils » 48
10.Onglet « Raccordements » 49
11.Onglet « Caractéristiques » 50
12.Supprimer/rajouter un lecteur 51
Les périphériques des centrales 52
1. Les modules d'extension d'entrées 52
Les périphériques des centrales 53
2.Création des groupes d'entrées 53
3.Les modules d'extension de sorties 54
4.Création des groupes de sorties 55
5.Les compteurs 56
6.Les Automatismes « Centrale » 57
Etat des centrales 60
Mettre à jour la centrale 62
Détection modules Ethernet 62
Les automatismes « centralisés » 63
1.Les compteurs globaux, Emails, Exportations et consignes 64
2.Édition des automatismes « Centralisés » 65
Les Zones contrôlées 68
Les droits d'accès 69
Les Groupes d'accès 70
Les plages horaires 71
1.Les plages horaires « Utilisateur » 71
2.Les plages horaires « Automatismes » 72
3.Les jours fériés 73
Les utilisateurs et les badges 74
Créer une nouvelle série de badges 75
Liste des badges/utilisateurs 76
Apprentissage des badges 77
Personnalisation du Badge 78
Modèle de badge imprimable 79
La fiche badge/utilisateur 80
1.Le profil « standard » 80
2.Les profils « additionnels » 81
3.L'onglet « Options » 82
4.L'onglet « Informations complémentaires » 83
5.L'onglet « Enrôlement » 84

6.L'onglet « Encodage »....85
7.L'onglet « Impression »....86
8.Récupération rapide des données....87
Les opérateurs du logiciel....88
Les profils des opérateurs....89
1.Créer un Profil....89
Les profils des opérateurs....90
2.Modifiez un Profil....90
3.Supprimer un profil....90
Les opérateurs....91
1.Créer un Opérateur....91
Les opérateurs....92
2.Modifier un Opérateur....92
3.Supprimer un Opérateur....92
Le journal de bord....93
Gestion Multi-société/Locataires....94
Les extensions « logiciel »....95
« Codes site » et « codes distributeur »....96
Préférences d'affichage....97
Gestion des Plugins....98
Gestion des fichiers XML....99
Activation de la gestion des caméras IP....101
Activation de la gestion des centrales d'alarme GALAXY....102
Rapport de configuration....103
Les applications « logiciel »....104
Configurer la sauvegarde automatique....106
Le temps de présence....107
Occupation des zones....108
Localiser un badge....109
Remise en cycle des badges....110
Pilotage des lecteurs....111
L'alarme Intrusion....112
1.Paramétrage des centrales....112
2.Ajouter des centrales d'alarme GALAXY....113
3.Modifier une centrale d'alarme GALAXY....114
4.Lancer la communication....115
5.Tracer le dialogue....115
6.Supprimer une centrale....115
7.Le simulateur....116

8.Afficher une centrale d'alarme GALAXY 117
9.Historique des alarmes 118
Levée de doute « Vidéo IP » 119
1.Ajouter une caméra 119
2.Modifier une caméra 119
3.Supprimer une caméra 119
4.Gestion des prépositions des dômes 120
5.Gestion des vues 121
6.Gestion des cycles 122
7.Enregistrements des photos/séquences vidéo 123
8.Rechercher les photos 124
9.Rechercher les séquences vidéo 125
Levée de doute « Vidéo via VDR» 126
1.Ajouter un DVR 126
2.Ajouter une caméra 126
3.Afficher les caméras 127
Gestion graphique du site 128
1.Ajouter un plan 128
2.Les composants 129
3.Ajouter les composants 130
4.Personnaliser les composants 131
5.La supervision 132
Liste des événements 133
1.Paramétrage des événements 133
2.Journal fil de l'eau 134
3.Les listes 135
Historique avancé 136
Assistance technique 139

Chapitre 1

Installer et utiliser « SENATORFX.NET®

Que contient ce chapitre ?

« Installer et utiliser « SENATORFX.NET® » 8
Éditions de SENATORFX.NET® 9
Exigences du logiciel SENATORFX.NET® 10
Installation du logiciel SENATORFX.NET® 11
Installation du logiciel SENATORFX.NET® (suite) 12
Démarrer le logiciel SENATORFX.NET® 13
Applications multipostes clients-serveurs 14
Les modules complémentaires 15

SENATORFX.NET® est un logiciel de gestion de contrôle d'accès intégré avancé et puissant.

Le chapitre qui suit contient d'importants renseignements concernant l'installation et l'utilisation de ce logiciel.

Installer et utiliser SENATORFX.NET®

Éditions de SENATORFX.NET®

Le logiciel SENATORFX.NET® existe en six éditions.

Références	Désignation	Multi postes
DONGLEFXCD2	Licence 2 lecteurs + CD-Rom **SENATORFX.net®** + **C1P2FXBT** (UTL 2 lecteurs)	10 postes
DONGLEFXCD16	Licence 16 lecteurs + CD-Rom logiciel **SENATORFX.net®**	10 postes
DONGLEFXCD64	Licence 64 lecteurs + CD-Rom logiciel **SENATORFX.net®**	10 postes
DONGLEFXCD512	Licence 512 lecteurs + CD-Rom logiciel **SENATORFX.net®**	10 postes
SENATORFX.NET64	kit comprenant **SENATORFX.net®** + licence 64 lecteurs + Interface **C485FX** + webcam	10 postes
SENATORFX.NET512	kit comprenant **SENATORFX.net®** + licence 512 lecteurs + Interface **C485FX** + webcam	10 postes

La licence du logiciel **SENATORFX.NET®** se présente sous forme d'une carte électronique appelée « Dongle » qui s'enfiche sur la carte mère d'une des centrales de l'installation.

La version « **DONGLEFXCD2** » permet la gestion de 2 lecteurs via une centrale **C1P2FXBT** sans nécessiter la licence.

Toutes les fonctionnalités sont intégrées quelque soit l'édition du logiciel.

La seule différence entre les éditions du logiciel **SENATORFX.NET®** est le nombre de lecteurs d'accès gérés.

Chaque édition permet une gestion multipostes « clients serveur » sans licence ou modules supplémentaires.

Références	Désignation	Multi postes
LIGALAXY	Licence de supervision des centrales d'alarme de la gamme Galaxy Dimension d'Honeywell	10 postes
LIAXISIP4	Licence de levée de doute et management pour 4 cameras IP (gamme Axis)	10 postes
LIDEV	Développement logiciel spécifique selon CCTP client	10 postes

Installer et utiliser SENATORFX.NET®

Exigences du logiciel SENATORFX.NET®

Le Serveur

Le serveur **SENATORFX.NET®** gère les centrales de gestion locales et entretient la base de données du système de contrôle d'accès intégré.

Le CD du logiciel **SENATORFX.NET®** comprend l'applicatif client-serveur, les différents drivers des modules biométriques nécessaires et compatibles.

Les différents manuels nécessaires à l'installation et l'utilisation du logiciel**SENATORFX.NET®** sont aussi disponibles sur le CD:

- Guide de démarrage rapide
- Aide en ligne
- Manuel de référence

Exigences de l'ordinateur (Serveur)

Le serveur est conçu pour fonctionner avec des ordinateurs de type PC utilisant un système d'exploitation Windows approprié tel que décrit dans « Exigences du système d'exploitation».

- Processeur cadencé à 2GHz
- 2Go de mémoire vive (4Go pour une performance optimum)
- 3Go d'espace disque dur libre recommandé; et plus pour les très grandes installations)
- 1 Port série RS-232 selon l'installation (et plus d'un port peut être nécessaire)
- 2 Ports USB disponibles minimum (et plus pour les très grandes installations)
- 1 Port Ethernet pour liaison réseau et mise à jour du logiciel via liaison Internet
- 1 carte graphique DirectX 9 accompagnée de 128 Mo de mémoire
- Moniteur de norme VGA

Exigences du système d'exploitation

Le serveur **SENATORFX.NET®** a été testé et validé sur les systèmes d'exploitation suivants :

- Windows® XP SP3 édition Familiale et Professionnelle
- Windows® 2003 SP2 édition Serveur
- Windows® Vista édition Familiale Basique, Familiale Premium, Entreprise et Intégrale
- Windows® 7 édition Professionnelle, Ultimate

Logiciels tiers nécessaires :

- Microsoft SQL Server 2005 Express (inclus sur le CD) ou supérieur
- Microsoft.NET Framework 3.5 (inclus sur le CD)

Installer et utiliser SENATORFX.NET®

Installation du logiciel SENATORFX.NET®

Insérez le CD-ROM **SENATORFX.NET®** dans votre lecteur et attendez l'exécution automatique de l'installation. Suivez alors les instructions qui s'affichent à l'écran.

Installez les drivers de la Webcam et celui du module biométrique si nécessaire

Pour installer le logiciel **SENATORFX.NET®**, il faut être connecté en tant qu'administrateur.

SenatorFX.NET - InstallShield Wizard
Welcome to the InstallShield Wizard for SenatorFX.NET
The InstallShield(R) Wizard will install SenatorFX.NET on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

SenatorFX.NET - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
PLEASE READ THIS LICENSE AGREEMENT IN ITS ENTIRETY. THEN CHOOSE EITHER "I AGREE" OR "I DO NOT AGREE" BELOW.
ACCORD DE LICENCE LOGICIELLE
1/ Accord de licence logicielle
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

1. **Acceptez le contrat de licence après l'avoir lu**.

SenatorFX.NET - InstallShield Wizard
Type of installation
Type of installation
Please select a type of installation
Full
Used to install all functions of the program: communication service, database and Man-Machine Interface. The communication service should be installed only once per site.
UI
Installs the Man-Machine Interface only. To be deployed on all workstations where SenatorFX.NET is to be installed, by connecting to the communication service.
InstallShield
< Précédent
Suivant >
Annuler

2. **Choix du type d'installation :**

Complète : Choisissez cette option pour installer le service de communication afin de pouvoir dialoguer avec
les centrales, la base de données, ainsi que l'interface graphique du logiciel

Client : Choisissez cette option pour vous connecter à un poste distant sur lequel est installé le service de communication.
N'installera que l'interface graphique du logiciel.

Installer et utiliser SENATORFX.NET®

Installation du logiciel SENATORFX.NET® (suite)

SenatorFX.NET - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

3. Confirmez le démarrage de l'installation en cliquant sur « Installer »

SenatorFX.NET Installer Information
You must restart your system for the configuration changes made to SenatorFX.NET to take effect. Click Yes to restart now or No if you plan to restart later.
Yes
No

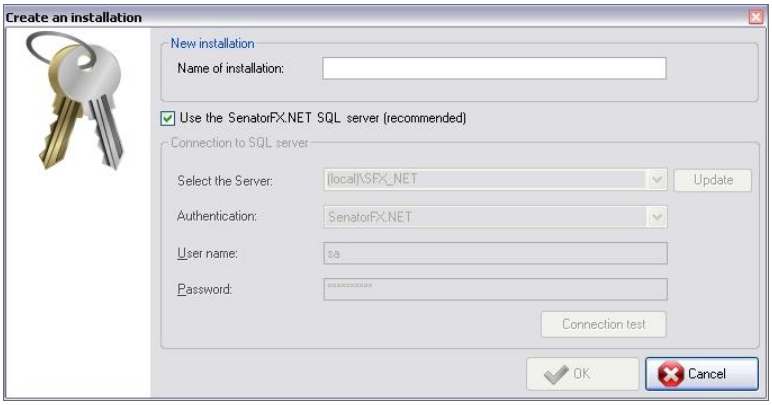
4. Redémarrez l'ordinateur

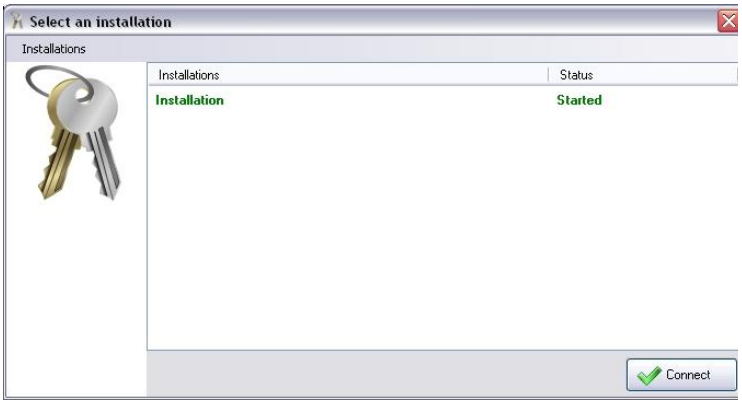
Si vous avez choisi une installation complète, un redémarrage de l'ordinateur est nécessaire

Installer et utiliser SENATORFX.NET®

Démarrer le logiciel SENATORFX.NET®

Premier lancement du serveur après avoir redémarré l'ordinateur





1. Entrez le nom de votre installation

La fenêtre de création d'une nouvelle installation apparaît.
Entrez le nom de votre installation puis cliquez sur *OK*.

2. Démarrez le service de communication

Une fois l'installation créée, sélectionnez la dans la liste des installations puis cliquez sur « *Connect* » pour démarrer le service de communication.
L'installation active apparaît en vert, vous pouvez alors fermer la fenêtre.

3. Lancez l'interface graphique

Cliquez sur le raccourci **SENATORFX.NET®** de votre bureau. L'écran de connexion apparaît.

Cliquez sur OK.

Par défaut, il n'y a pas de mot de passe pour le profil « ADMINISTRATEUR ».
Par la suite il est conseillé de créer un mot de passe pour accéder au logiciel.

4. Ouverture de la page principale du logiciel SENATORFX.NET®

Vous avez accès à l'interface principale du logiciel, avec le ruban des menus sur la gauche, et l'espace de travail sur la droite.

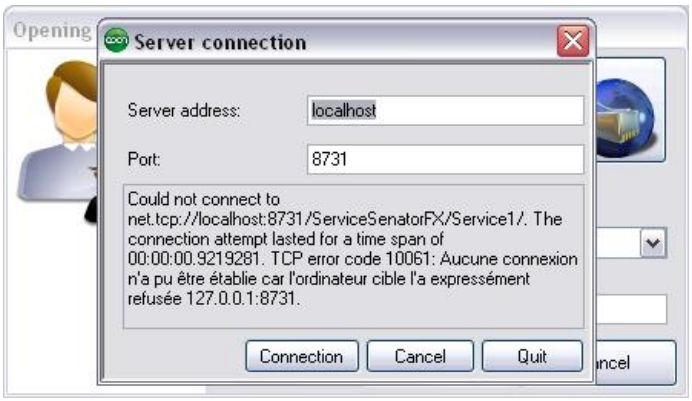
Installer et utiliser SENATORFX.NET®

Applications multipostes clients-serveurs

SENATORFX.NET® permet à plusieurs PC (jusque 10 postes clients) sur un même réseau de gérer une même installation sans aucun besoin de licence supplémentaire.

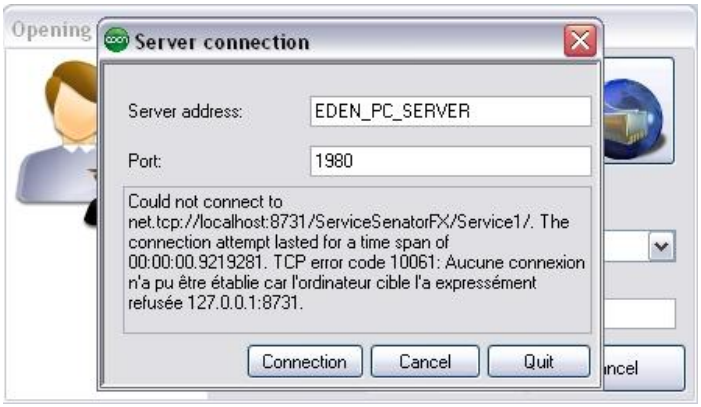
Sur les postes distants, choisissez « Client » dans le choix du type d'installation : se reporter au chapitre « Installation logiciel » pour plus de détails.

Lors du premier démarrage du poste client, procédez comme suit :


Opening
Server connection
Server address:
localhost
Port:
8731
Could not connect to net.tcp://localhost:8731/ServiceSenatorFX/Service1/. The connection attempt lasted for a time span of 00:00:00.9219281. TCP error code 10061: Aucune connexion n'a pu être établie car l'ordinateur cible l'a expressément refusée 127.0.0.1:8731.
Connection
Cancel
Quit

Par défaut, l'interface graphique essaye de se connecter au serveur sur le poste courant.

2. Cliquez sur *OK.*


Opening
Server connection
Server address:
EDEN_PC_SERVER
Port:
1980
Could not connect to net.tcp://localhost:8731/ServiceSenatorFX/Service1/. The connection attempt lasted for a time span of 00:00:00.9219281. TCP error code 10061: Aucune connexion n'a pu être établie car l'ordinateur cible l'a expressément refusée 127.0.0.1:8731.
Connection
Cancel
Quit

1. Précisez le nom du poste sur lequel est installé le service de communication

Vous devez préciser dans le champ ***Adresse du serveur*** le nom du poste (ou son adresse IP si celle-ci est fixe) sur lequel est installé le service de communication. Cliquez sur ***Connexion***.

3. Ouverture de la page principale du logiciel SENATORFX.NET®

Le logiciel sortira du mode « Démo » lors de la reconnaissance de la présence de la licence « Dongle » enfiché sur une des centrales de l'installation (voir Editions de SenatorFX.NET page 9)

Si vous ne parvenez pas à passer l'écran Connexion Serveur :

- Assurez-vous que le service de communication est à l'état démarré sur le poste serveur
- Assurez-vous de la valeur entrée pour le champ adresse du serveur
- Assurez-vous que le port 8731 est utilisé par défaut
- Assurez-vous qu'il n'a pas été modifié sur le poste serveur
- Si un pare-feu est actif sur le poste serveur, il faut ajouter une exception TCP pour le port 8731.

Installer et utiliser SENATORFX.NET®

Les modules complémentaires

SENATORFX.NET® permet d'intégrer d'autres solutions de sécurité complémentaires à la gestion du contrôle d'accès:

- La supervision des alarmes Intrusion avec les centrales « GALAXY Dimension » du constructeur HONEYWELL
- La levée de doute vidéo avec les caméras et dômes IP du constructeur AXIS

Se reporter à la procédure d'installation des modules « Plug-in » pour de plus amples informations.

Pour profiter des modules complémentaires, veuillez vous assurer que l'installation bénéficie d'une licence « Dongle ». Cette licence s'affiche en bas à droite de l'écran du logiciel.

Chapitre 2

Interface utilisateur de SENATORFX.NET

Que contient ce chapitre ?

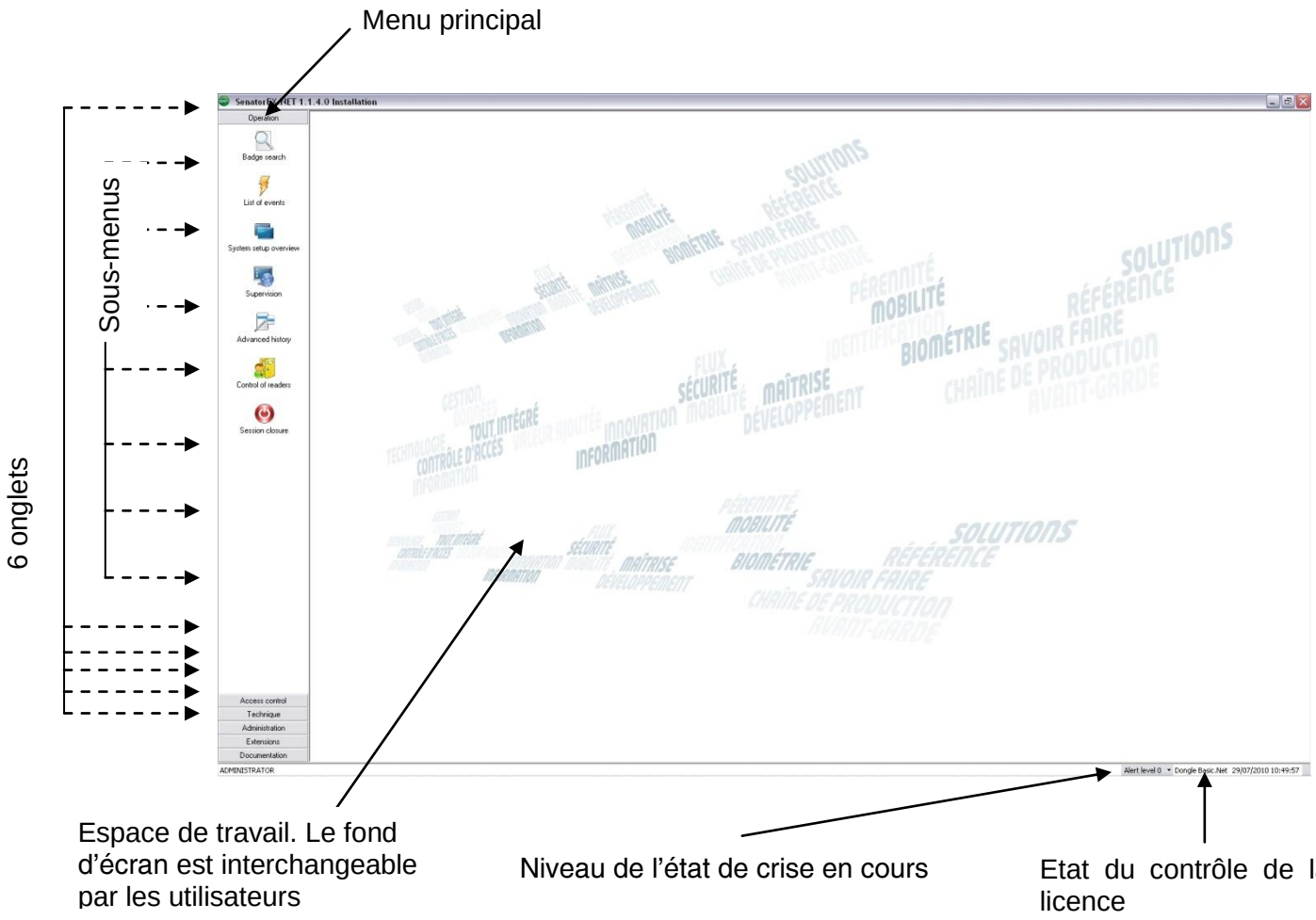
Interface utilisateur de SENATORFX.NET 16
Survol de l'écran principal 17
Onglet et sous menus « Exploitation » 18
Onglet et sous menus « Contrôle d'accès » 19
Onglet et sous menus « Technique » 20
Onglet « Administration » et ses sous menus 20
Onglet et sous menus « Extensions » 21
Onglet et sous menus « Documentation » 22

Ce chapitre présente la structure de la fenêtre principale ainsi que les différents menus, onglets, et sous-menus de l'application.

Interface utilisateur de SENATORFX.NET®

Survol de l'écran principal

Le menu principal du logiciel est présenté sur une colonne verticale via 6 onglets.



Certains sous-menus peuvent ne pas apparaitre selon les droits d'accès de l'opérateur et/ou l'absence de modules complémentaires du logiciel **SENATORFX.NET®.**

Les 6 onglets du menu principal

Interface utilisateur de SENATORFX.NET®

Onglet et sous menus « Exploitation »

Icônes	Onglet « Exploitation »	Description
	Recherche de badge	Edition, recherche et gestion des badges et identifiants du site
	Liste des événements	Monitoring temps réel des événements du contrôle d'accès et des alarmes Intrusion
	Éditeur synoptique	Éditeur des plans graphiques (BMP/JPG) avec icones pour la supervision
	Supervision	Gestion graphique « temps réel » via plans dynamiques du site
	Historique avancé	Outil de requête historique sur les événements.
	Listing absents	Gestion « temps réel » des présents et absents sur site
	Caméras IP	Module de levée de doute vidéo pour caméras et dômes IP
	Alarme Intrusion GALAXY	Module de gestion et supervision des centrales d'alarme Intrusion GALAXY d'HONEYWELL
	Pilotage des lecteurs	Contrôle et pilotage des accès au site
	Fermeture de la session	Fermeture de session pour déconnecter l'opérateur

Certains sous-menus peuvent ne pas apparaitre selon les droits d'accès de l'opérateur et/ou l'absence de modules complémentaires du logiciel **SENATORFX.NET®.**

Interface utilisateur de SENATORFX.NET®

Onglet et sous menus « Contrôle d'accès »

Icônes	Onglet « Contrôle d'accès »	Description
	Groupes d'accès	Edition des groupes d'utilisateurs
	Plages horaires	Édition des programmes hebdomadaires et périodes de jours fériés/spéciaux
	Badges	Édition et gestion des fiches « badge/utilisateur »
	Apprentissage	Enrôlement des badges via apprentissage avec choix du lecteur
	Personnalisation des badges	Éditions des champs complémentaires des fiches « badge/utilisateur »
	Paramétrages des événements	Configuration de l'affichage des événements dans la liste des événements
	Listes	Édition de listes d'événements « temps réel » avec choix de filtres
	Zones contrôlées	Édition de zones avec lecteurs « Entrée/Sortie » pour présence et comptage
	Automatismes centralisés	Édition de scénarios d'automatisme managés par le logiciel « On-line »
	Rapport de configuration	Impression du paramétrage complet du site

Certains sous-menus peuvent ne pas apparaitre selon les droits d'accès de l'opérateur et/ou l'absence de modules complémentaires du logiciel **SENATORFX.NET®.**

Interface utilisateur de SENATORFX.NET®

Onglet et sous menus « Technique »

Icônes	Onglet « Technique »	Description
	Configuration du site	Edition et création des centrales, lecteurs et périphériques du site
	État des centrales	Gestion temps réel du statut des centrales de l'installation
	Mettre à jour la centrale	Mise à jour du Firmware des centrales de gestion
	Détection modules Ethernet	Détection et modification automatique des modules de liaison réseau Ethernet EDEN

Onglet « Administration » et ses sous menus

Icônes	Onglet «Administration»	Description
	Profils d'utilisateurs	Gestion des droits d'accès des opérateurs du logiciel
	Utilisateurs	Gestion des opérateurs du logiciel via mot de passe et profil
	Journal de bord	Historique des actions effectuées par les opérateurs du logiciel
	Sociétés	Édition des sociétés ou locataires du site
	Récupération rapide des données	Module d'importation de bases de données au format texte ou tableur

Certains sous-menus peuvent ne pas apparaitre selon les droits d'accès de l'opérateur et/ou l'absence de modules complémentaires du logiciel **SENATORFX.NET®.**

Interface utilisateur de SENATORFX.NET®

Onglet et sous menus « Extensions »

Icônes	Onglet « Extension»	Description
	Temps de présence	Module de « cumul de temps de présence » dans les zones du site
	Enregistreur vidéo	Management des enregistreurs vidéo tiers Dedicated Micros et Bosch
	Occupation des zones	Affichage et impression de l'occupation des zones du site
	Localiser un badge	Rechercher un badge/utilisateur et afficher son dernier point de passage
	Code site	Gestion des codes « site » des badges permettant un niveau de sécurité supérieur
	Code distributeur	Gestion des codes « distributeur » des badges permettant un niveau de sécurité supplémentaire
	Configurer la sauvegarde automatique	Édition du rappel de la sauvegarde de la base de données du site
	Préférences	Gestion d'affichage et des modules complémentaires du logiciel SENATORFX.NET
	Remise en cycle des badges	Remise en cycle de l'Anti-Passback (Anti-retour) des badges du site

Certains sous-menus peuvent ne pas apparaitre selon les droits d'accès de l'opérateur et/ou l'absence de modules complémentaires du logiciel **SENATORFX.NET®.**

Interface utilisateur de SENATORFX.NET®

Onglet et sous menus « Documentation »

Icônes	Onglet «Documentation»	Description
	Notice d'utilisation et d'installation	Manuel d'utilisation en ligne du logiciel
	Bloc notes	Editeur de texte libre
	À propos	Version du logiciel installé
	Mises à jour	Module de mise à jour du logiciel via liaison Internet via serveur EDEN

Certains sous-menus peuvent ne pas apparaitre selon les droits d'accès de l'opérateur et/ou l'absence de modules complémentaires du logiciel **SENATORFX.NET®.**

Chapitre 3

Configuration du site

Que contient ce chapitre ?

Configuration du site 23
Création d'une installation 25
Gestion des bases de données 26
Le service Controller 27
Les réseaux de centrales 28
1.Ajouter un réseau 28
2.Création d'un réseau via liaison « Port Com » 29
3.Création d'un réseau via liaison « Port USB » 29
4.Création d'un réseau via liaison « Port Ethernet » 30
5.Modification/supression d'un réseau 31
6.Utilisation de la biométrie 32
Paramétrage des centrales 34
1.Création /modification d'une centrale 34
2.Dupliquer une centrale 38
3.Supprimer une centrale 39
Paramétrage des lecteurs 40
1.Configurer le type de lecteur 40
2.Détection automatique du format de badges existant 43
3.La biométrie 44
4.Paramétrer un lecteur 45
5.Onglet « Fonctions standards » 46
6.Onglet « Fonctions spéciales » 47
7.Onglet « Profils » 48
8.Onglet « Raccordements » 49
9.Onglet « Caractéristiques » 50
10.Supprimer/rajouter un lecteur 51
Les périphériques des centrales 52
1.Les modules d'extension d'entrées 52
Les périphériques des centrales 53
2.Création des groupes d'entrées 53
3.Les modules d'extension de sorties 54
4.Création des groupes de sorties 55
5.Les compteurs 56
6.Les Automatismes « Centrale » 57
Etat des centrales 60

Mettre à jour la centrale 62
Détection modules Ethernet 62
Les automatismes « centralisés » 63
1. Les compteurs globaux, Emails, Exportations et consignes 64
2.Édition des automatismes « Centralisés » 65
Les Zones contrôlées 68

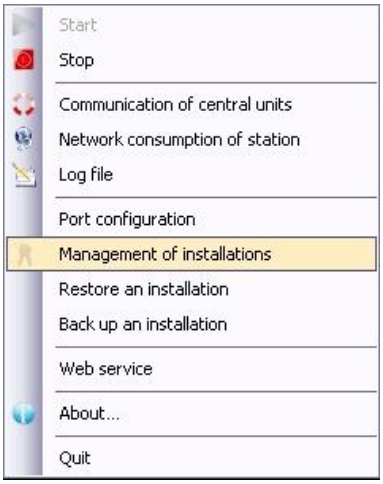
Configuration du site

Création d'une installation

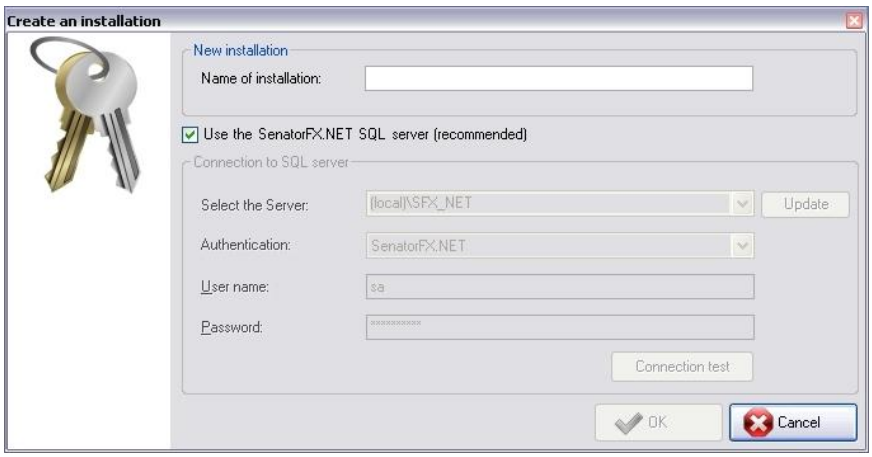
La création du site démarre avec la création d'une installation. La création d'une installation génère une nouvelle base de données qui sera stockée sur le serveur principal.

Cette base de données est au format SQL SERVER Express 2005 par défaut, mais une autre instance peut être choisie en décochant la case « Utiliser le serveur SenatorFX.NET ».

La gestion des installations est possible grâce à l'application "Service Controller" accessible depuis la zone de tâches Windows.



1. Cliquez sur « gestion des installations »

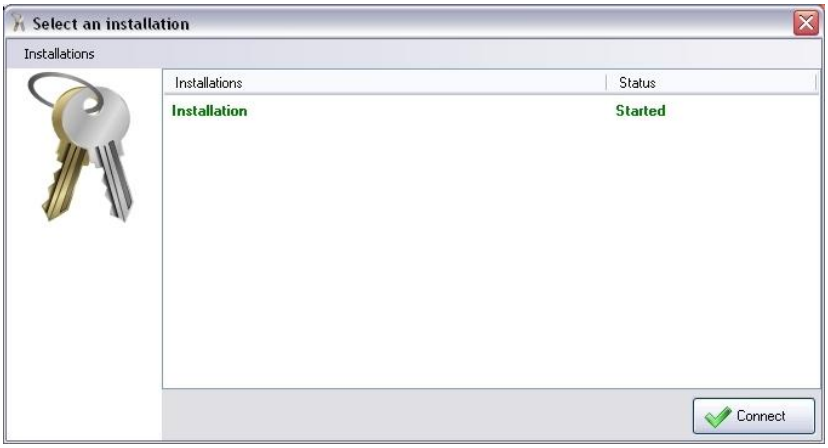


2. Entrez le nom de votre installation

La fenêtre de création d'une nouvelle installation apparaît. Entrez le nom de votre installation puis cliquez sur *OK*.

3. Sélectionnez la nouvelle installation

Une fois l'installation créée, sélectionnez la dans la liste des installations, puis cliquez sur « *Connect* » pour démarrer le service de communication.
L'installation active apparaît en vert, vous pouvez alors fermer la fenêtre.



Informations relatives aux installations :

- Elles ne peuvent être gérées qu'à partir du poste serveur
- Une seule installation peut être active sur un poste
- Une installation représente tous les paramétrages relatifs à un site
- Les installations sont complètement indépendantes les unes des autres

Repérez l'icône du service Controller dans la zone de tâches

indique que le service SenatorFX.NET est en cours d'exécution

indique que le service SenatorFX.NET est en cours de démarrage

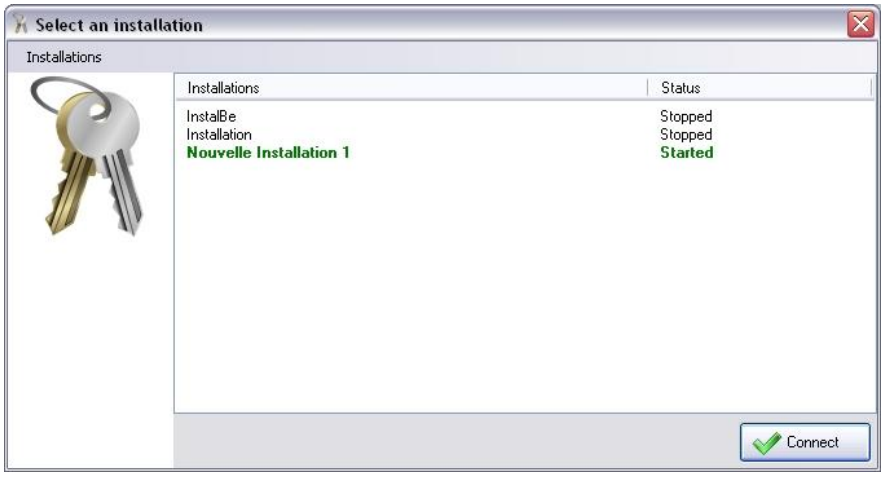
indique que le service SenatorFX.NET est en cours d'arrêt

indique que le service SenatorFX.NET est arrêté

Configuration du site

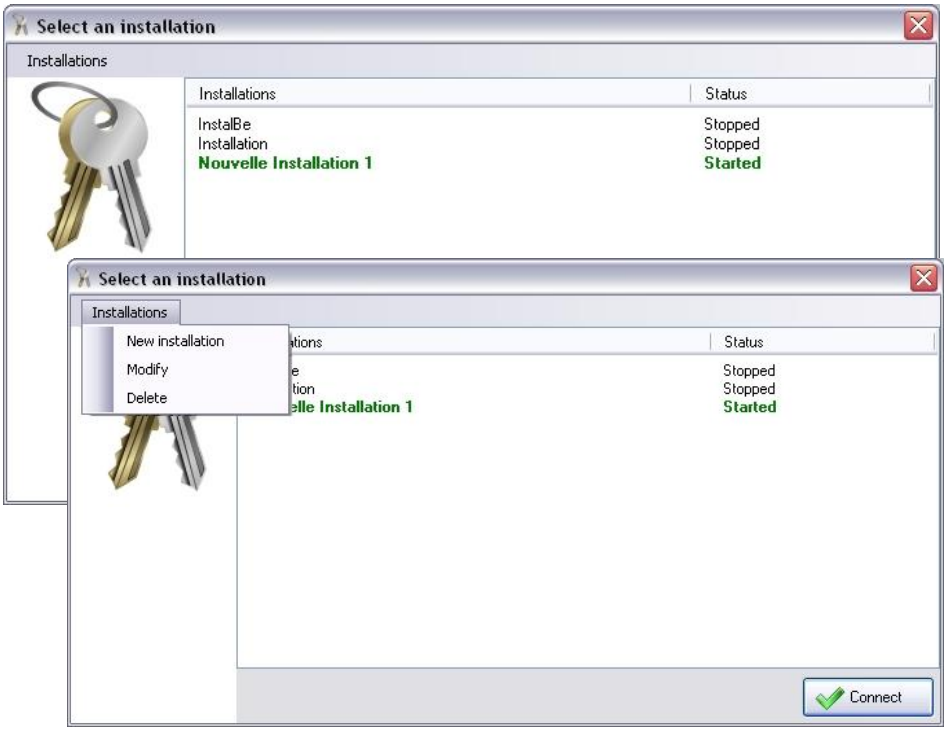
Gestion des bases de données

Cliquez sur "Gestion des Installations", la fenêtre suivante apparaît :



Dans l'exemple ci-dessus, une installation est activée, il s'agit de "Nouvelle Installation 1". Deux autres installations ont été créées : "Installation" et "InstallBe".
Tous les postes clients qui se connecteront à ce service dialogueront avec " Nouvelle Installation 1".
Pour modifier l'installation active, cliquez dessus, puis cliquez sur le bouton "***Déconnecter***"

De la même manière, pour activer une autre installation, cliquez dessus puis cliquez sur le bouton "Connecter".
Vous pouvez également créer, modifier ou supprimer une installation en vous servant du menu "Installations"



Configuration du site

Le service Controller

Menu du service Controller

Les options :

Démarrer : permet de démarrer le service en activant la dernière installation qui a été activée. Si aucune installation n'a été activée, ce choix n'a aucun effet.

Arrêter : permet d'arrêter le service. Cela a pour double effet d'interrompre la communication avec les centrales et de déconnecter tous les postes clients connectés au service.

Communication des centrales : affiche les échanges de trames entre le service et les centrales.

Consommation réseau du poste : affiche à titre indicatif la consommation réseau du poste. Il est à noter qu'il s'agit de la consommation général du poste et non pas uniquement celle de **SenatorFX.NET.**

Fichier de Log : affiche un fichier des messages renvoyés par le service **SenatorFX.NET.**

Configuration du port : permet de modifier le port sur lequel le service va dialoguer avec les postes clients.

Gestion des installations : permet de gérer les différentes installations. Voir plus haut.

Restaurer une installation : permet de restaurer une installation qui a été préalablement sauvegardée.

Sauvegarder une installation : permet de sauvegarder une installation; une sauvegarde comprend un backup de la base de données, ainsi que les fichiers externes : photos, plan de synoptiques, fichiers audio etc...

Quitter : arrête le service SenatorFX.NET et le service Controller. Pour redémarrer le service Controller, rendez-vous dans "Programmes/Eden/Service Controller".

Configuration du site

Les réseaux de centrales

Sélectionnez le menu « Technique », puis allez dans l'onglet « Configuration du site », « Réseau» et « Créer un réseau ».

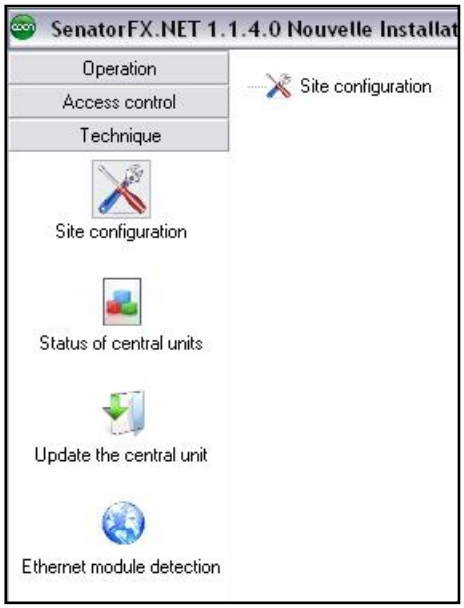
1. Ajouter un réseau

La création du site démarre avec la création d'un réseau. Un réseau peut comprendre une seule ou plusieurs centrales.

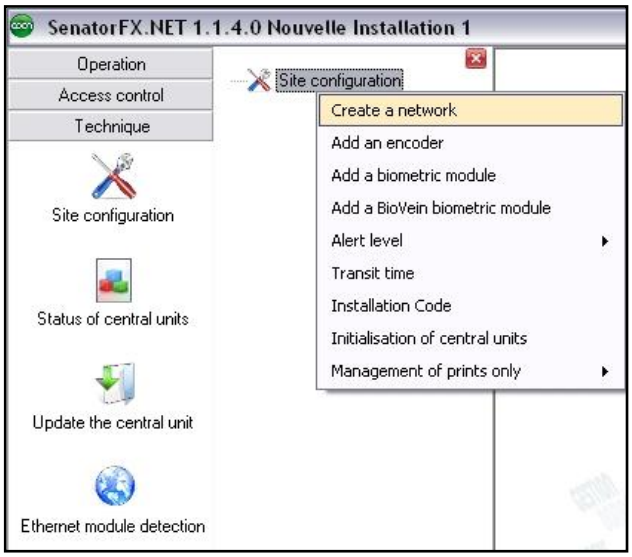
Chaque réseau peut être relié à l'ordinateur central ou serveur via plusieurs types de liaisons distinctes :

- Liaison « USB » via l'interface **C485FX**
- Liaison « Port COM RS232 » via l'interface **C485FX**
- Liaison « Ethernet » d'une seule centrale avec module **MODTCP/IP**
- Liaison « Ethernet » de plusieurs centrales avec l'interface **C485FX** + module enfichable **MODTCP/IP**

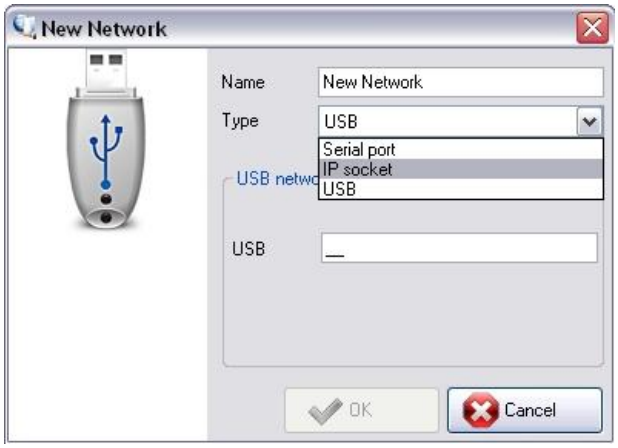
La création d'un réseau s'effectue via le menu Technique → Configuration du site.



1. Cliquez sur « Configuration du site »



2. Cliquez sur « Créer un réseau »



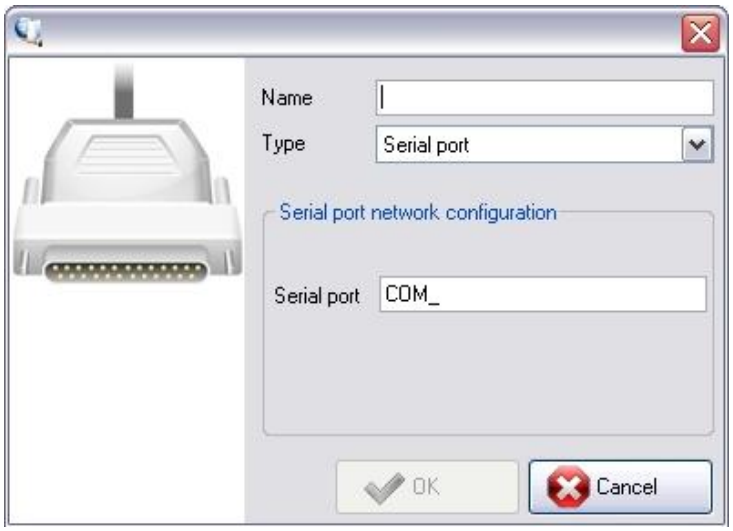
Configuration du site

Les réseaux de centrales

Sélectionnez le menu Technique → Configuration du site → Réseau → Créez un réseau

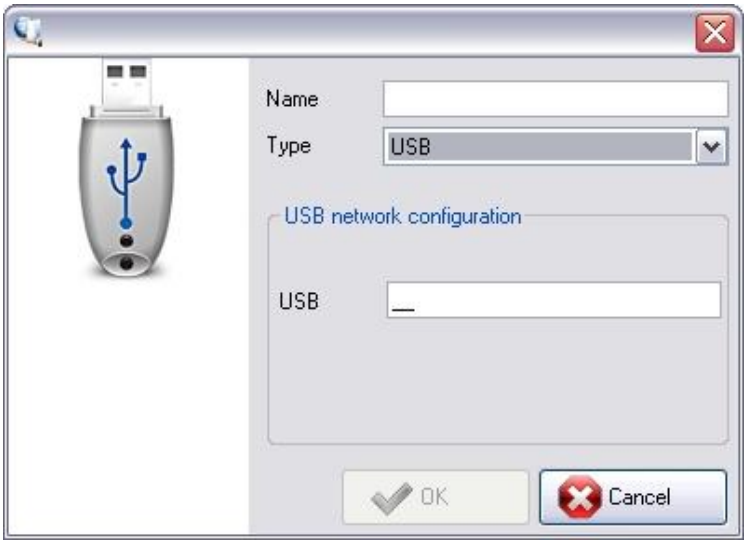
2. Création d'un réseau via liaison « Port Com »

Lorsque le réseau avec liaison « port SERIE » est choisi, la fenêtre ci-dessus apparait.



1. **Editez le nom du réseau dans le champ « Libellé »**
2. **Editez le numéro du port dans le champ « Port série »**

3. Création d'un réseau via liaison « Port USB »



1. **Editez le nom du réseau dans le champ « Libellé »**
2. **Editez le numéro du port dans le champ « Port USB »**

Configuration du site

Les réseaux de centrales

Sélectionnez le menu Technique → Configuration du site

4. Création d'un réseau via liaison « Port Ethernet »

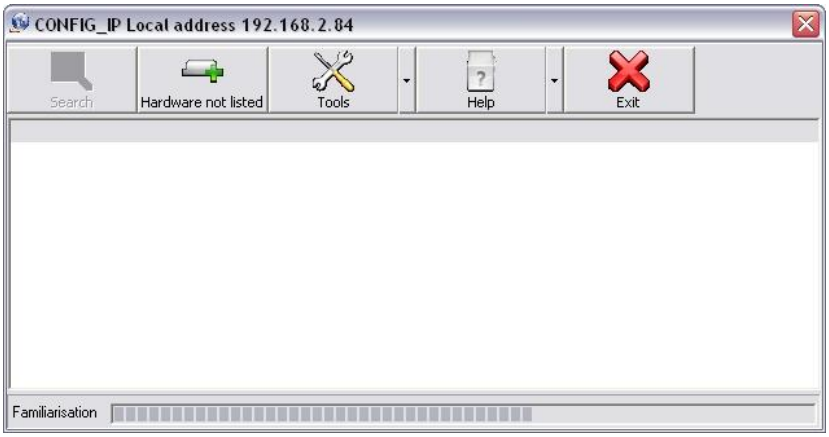
Lorsque le réseau avec liaison « port Ethernet » est choisi, la fenêtre ci-dessus apparait :

1. Editez le nom du réseau dans le champ « Libellé »

2. Editez l'adresse IP et le port dans le champ « Adresse »

Il est possible de choisir entre une adresse IP et une adresse DNS. Le champ « Adresse IP » est divisé en 2 parties par un « - ». La première partie permet d'entrer l'adresse IP et la seconde le port.

Il en va de même dans le cas d'un serveur DNS. Les ports par défaut sont, « 10001 » pour les Mod TCP/IP et « 04000 » pour les Comète-FX.



Le bouton « Rechercher » lance l'application « Config IP » qui permet la détection automatique du matériel présent sur le réseau Ethernet.

Note :

Il est possible d'effectuer l'action « glisser/déposer » de l'adresse IP, à partir de la fenêtre « Config IP » vers le champ « Adresse IP » de la fenêtre « Réseau ».

Le champ se remplit alors automatiquement.

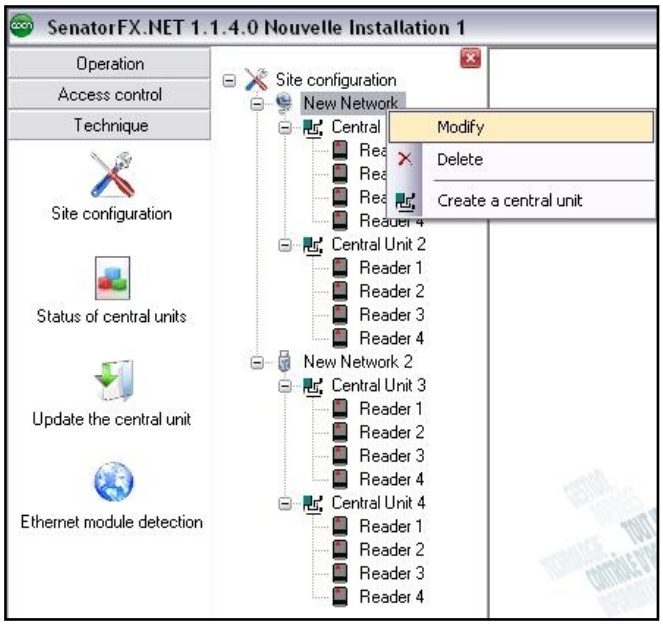
Configuration du site

Les réseaux de centrales

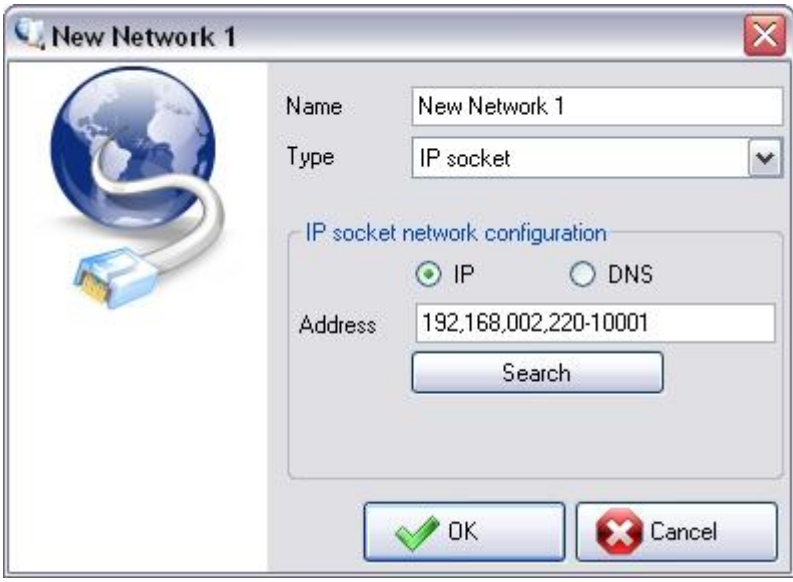
Sélectionnez le menu Technique → Configuration du site → Modification/Suppression d'un réseau.

5. Modification/suppression d'un réseau

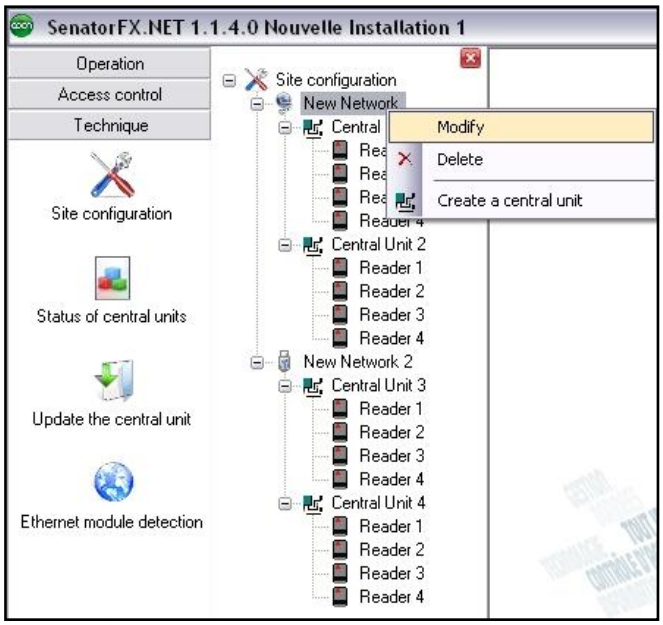
Pour modifier la technologie du réseau son adresse ou son libellé, utiliser « Modifier »



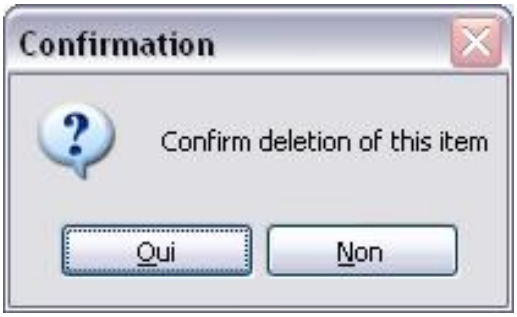
1. Sélectionnez le réseau de centrales à modifier



2. Modifiez les informations souhaitées



1. Pour supprimer un réseau de centrale, utilisez « Supprimer »



2. Confirmez la suppression du réseau de centrale

Nota: La suppression du réseau entrainera la suppression de toutes les centrales et autres périphériques associées

Configuration du site

Les réseaux de centrales

Sélectionnez le menu Technique → Configuration du site

6. Utilisation de la biométrie

Si vous utilisez des lecteurs de technologie biométrique, vous devez lire attentivement ce sous-chapitre. Il existe deux technologies

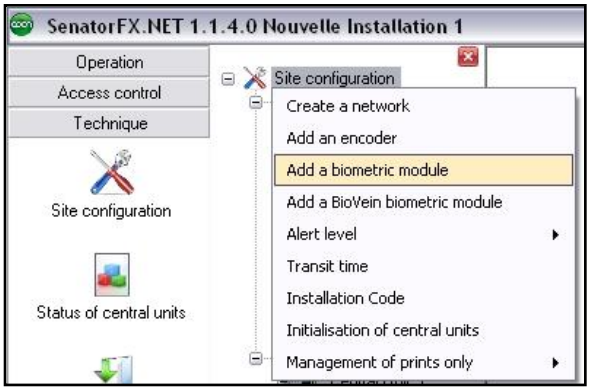
- La reconnaissance de l'empreinte digitale via les lecteurs « **SOLO** »
- La reconnaissance du réseau veineux du doigt via les lecteurs « **BIOVEIN** »

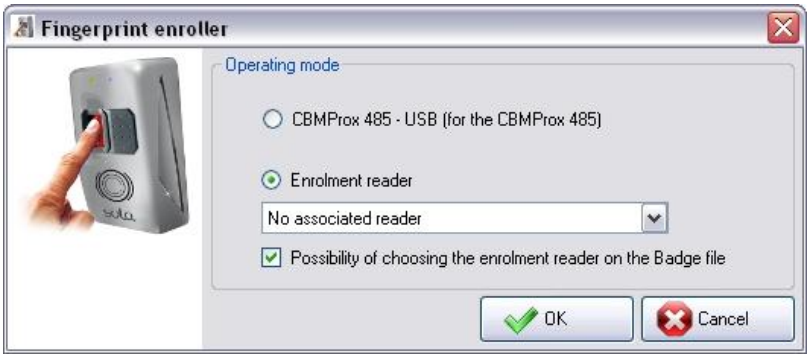
Vous devez créer un lecteur d'enrôlement par technologie utilisée.

Dans le cas d'une utilisation en badge + empreinte, le lecteur SOLO permet de respecter les préconisations énoncées par la CNIL dans sa délibération N°2006-102 du 17 avril 2006.

Il est nécessaire d'utiliser un encodeur de badges Mifare « **ENCODUSB** ».

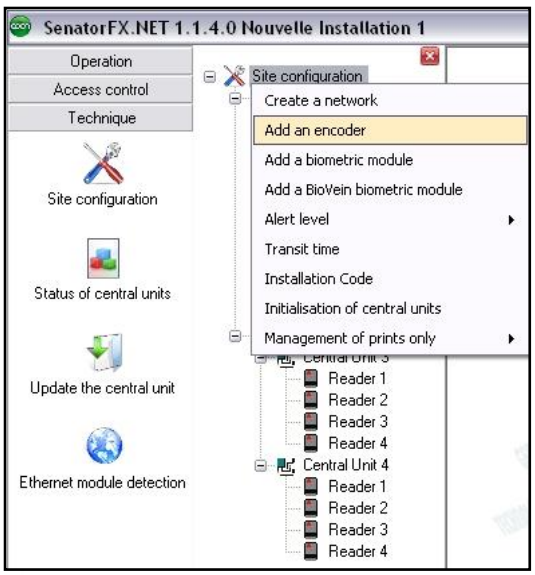
Création d'un lecteur d'enrôlement de technologie « Empreinte digitale »

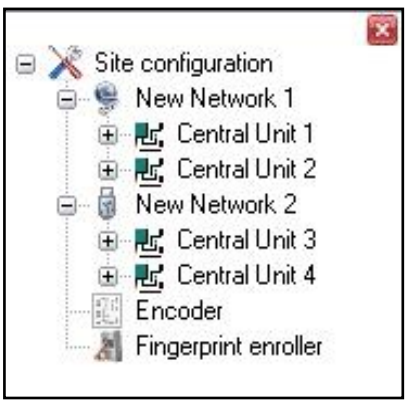




Sélectionnez le lecteur d'enrôlement avec liaison PC/USB ou un des lecteurs « SOLOS » du site

Création d'un lecteur d'enrôlement de technologie « Empreinte digitale »

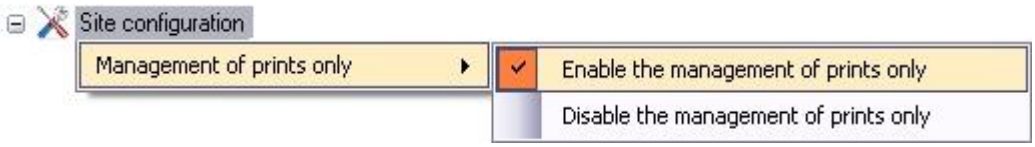




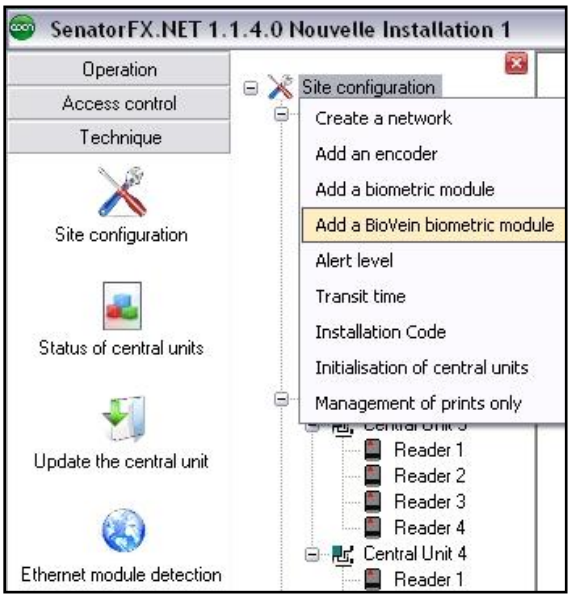
Configuration du site

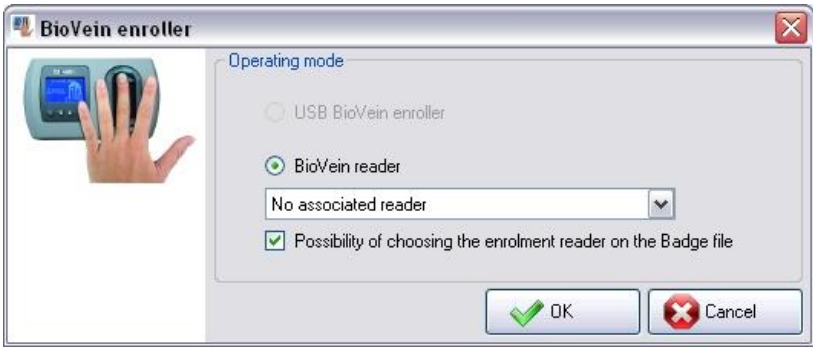
Les réseaux de centrales

Utilisation des empreintes digitale en mode « empreinte seule » (1 contre N)

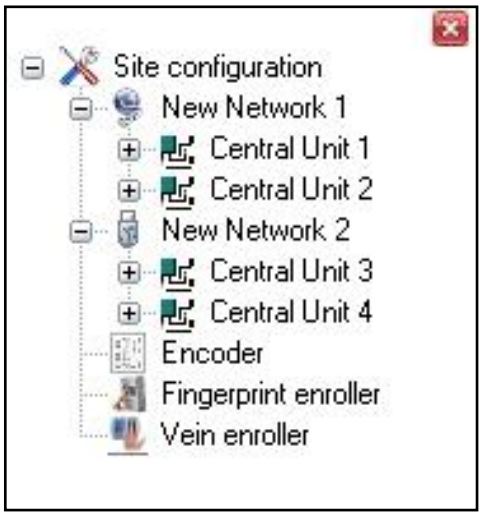

Site configuration
Management of prints only
Enable the management of prints only
Disable the management of prints only

Création d'un lecteur d'enrôlement de technologie « réseau veineux »





1. **Sélectionnez le lecteur d'enrôlement avec liaison PC/USB ou un des lecteurs « BIOVEIN » du site**



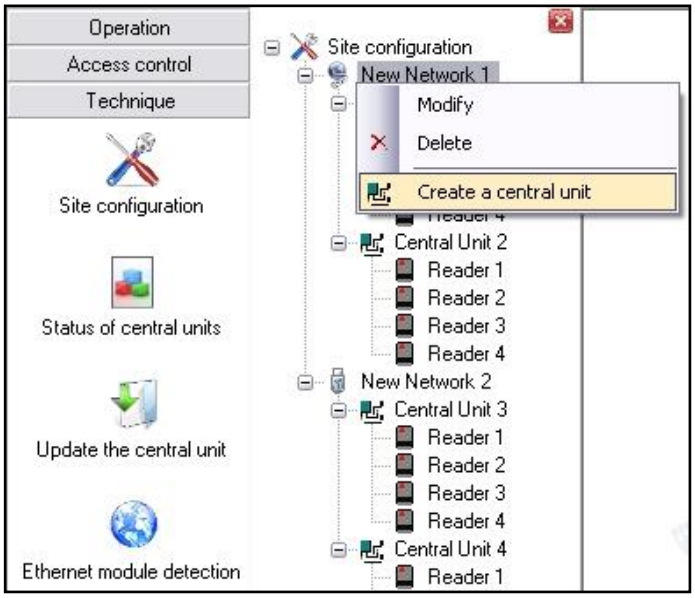
2. **L'enrôleur apparaît alors dans le synoptique de l'installation.**

Configuration du site

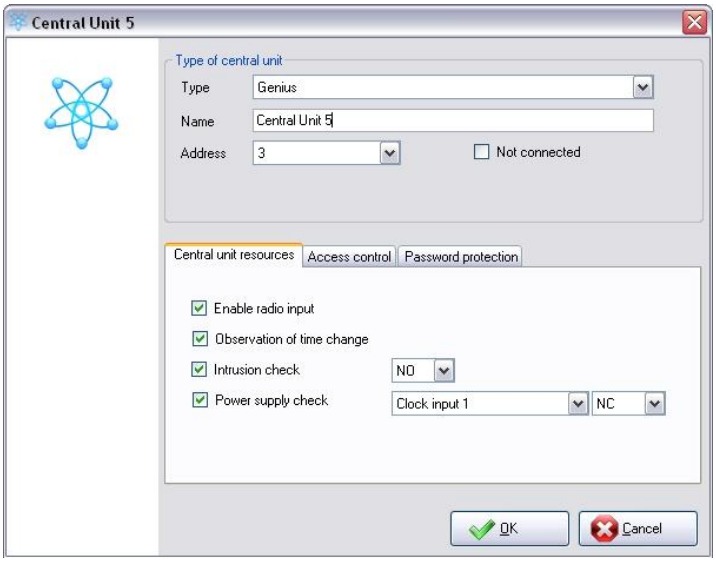
Paramétrage des centrales

Sélectionnez l'onglet « Technique » → Configuration du site

1. Création /modification d'une centrale



1. Sélectionnez le réseau et cliquez sur « créer une centrale »



2. Définir le modèle de centrale à éditer

- Utilisez le champ « Type de centrale »
- Faites dérouler le menu
- Sélectionnez la centrale

Tableau de rappel des centrales disponibles :

Référence	Modèle	Lecteurs	Technologies compatible	Liaisons	Identifiants
GENIUS	Centrale	2	Wiegand, Clock/data, Biométrie EDEN (RS485)	USB/RS485 Ethernet	10K
C1P2FX	Centrale	2	Wiegand, Clock/data, Biométrie EDEN (RS485)	USB/RS485 Ethernet	10K
C4PLUSFX	Centrale	4	Wiegand, Clock/data, Biométrie EDEN (RS485)	USB/RS485 Ethernet	10K
BIOVEIN	Lecteur biométrique	1	Veines du doigt	RS485 Ethernet	1K

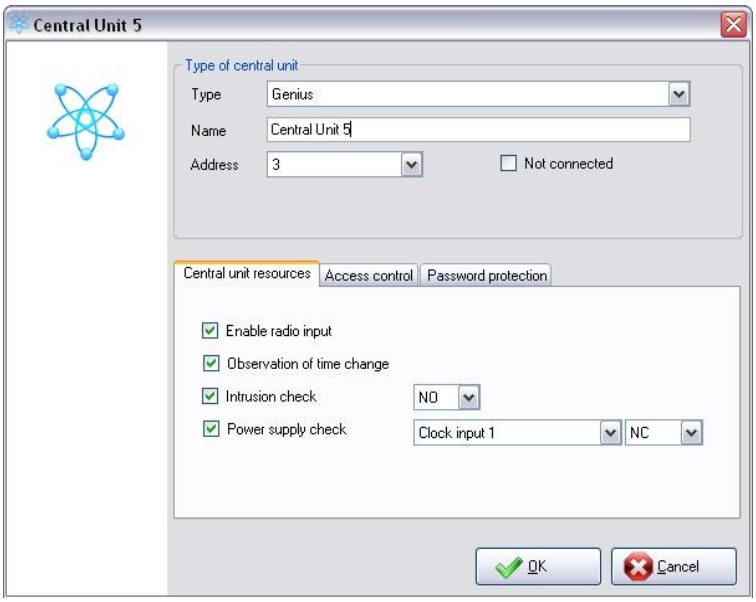
Paramétrage des centrales (suite)

1. Création d'une centrale (suite)

Pour nommer la centrale sous lequel, elle apparaitra dans le logiciel, il faut utiliser le champ « Libellé ».
Le menu déroulant « Adresse » permet de paramétrer l'adresse de la centrale dans le réseau.
Les adresses déjà utilisées sur le réseau n'apparaissent pas dans le menu déroulant.

Il est possible de mettre jusqu'à 32 centrales sur un même réseau. Les adresses disponibles sont donc celle de 1 à 32. La case « Hors connexion », lorsqu'elle est cochée, indique au logiciel de ne pas communiquer avec la centrale.

Descriptions de l'onglet « Ressources de la centrale » pour GENIUS, C1P2FX et C4PLUSFX



- Activez ou non « l'entrée radio »
- Activez le changement d'heure « été / hiver »
- Activez ou non « le contrôle Effraction »
- Choisissez le mode de l'entrée « ON ou OFF »
- Activez ou non « le contrôle Alimentation »
- Sélectionnez l'entrée de la centrale

Validez par « OK » quand les réglages sont terminés

Les centrales **GENIUS**, **C1P2FX** et **C4PLUSFX** disposent d'une entrée radio.
Cette entrée est compatible avec certains récepteurs radio de type **TECHNOEM** et **JCM**.

Pour activer cette entrée, il faut cocher la case « Activer entrée radio ».

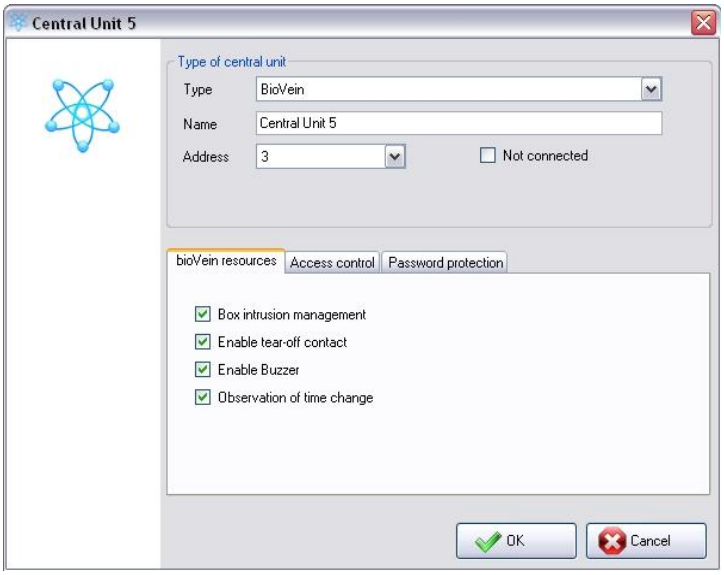
L'observation du changement d'heure » été/hiver permet une autogestion locale du lecteur sans connexion avec le logiciel et l'ordinateur.

Descriptions de l'onglet « **Ressources de la centrale** » pour **BIOVEIN**

- Activez ou non la gestion de l'effraction boitier
- Activez ou non « le contact d'arrachement »
- Activez le changement d'heure « été / hiver »
- Activez ou non « le buzzer du lecteur »

Validez par « OK » quand les réglages sont terminés

Le lecteur BIOVEIN permet la gestion de l'auto-protection du boîtier à l'ouverture et à l'arrachement. Cela peut générer une alarme locale ou déportée et bloquer l'utilisation du lecteur.
La fonction « buzzer » permet un acquit sonore lors de l'utilisation du lecteur.
L'observation du changement d'heure » été/hiver permet une gestion locale du lecteur sans connexion avec le logiciel et l'ordinateur.

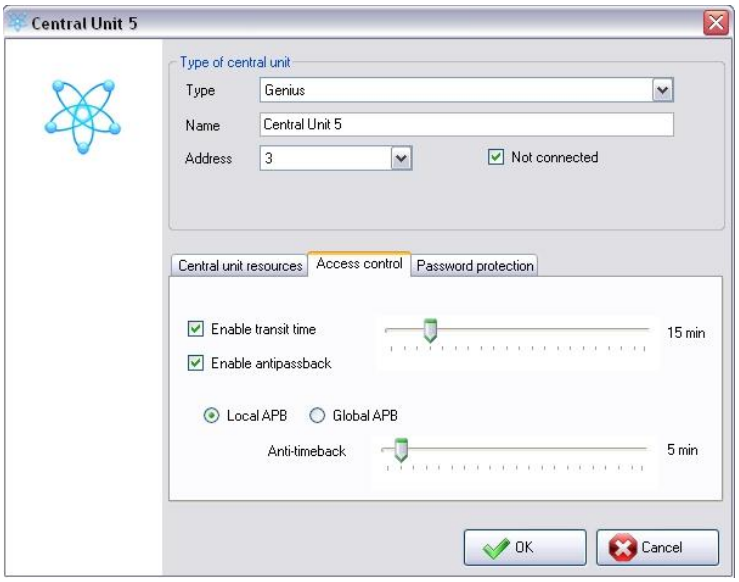


Configuration du site

Paramétrage des centrales (suite)

1. Création d'une centrale (suite)

Description de l'onglet « **Contrôle d'accès** » pour **GENIUS**, **C1P2FX** et **C4PLUSFX**



- Activez ou non « le délai de transit »
- Sélectionnez la durée du délai
- Activez ou non « l'Anti-passback »
- Choisissez le mode « local » ou le mode « global »
- Activez ou non « l'Anti-timeback »
- Sélectionnez la durée de « l'Anti-timeback »

- Validez par « OK » quand les réglages sont terminés

Lorsque l'on active « l'anti-passback », les options « APB Local », « APB Global » et « Anti-timeback » apparaissent.

Pour que la fonction d'anti-passback fonctionne, il faut au moins qu'un lecteur soit défini en entrée et un lecteur défini en sorti sur la centrale.

La centrale interdit alors à un même badge de passer 2 fois sur une entrée sans être passé par une sortie entre les 2 entrées, ou, inversement de passer 2 fois sur une sortie sans être passé sur une entrée entre les 2 sorties.

L' « APB Local » (Anti-Passback Local) permet d'activer la fonction anti-passback entre des accès d'une même centrale.

L' « APB Global » (Anti-Passback Global) permet d'activer la fonction anti-passback entre tous les accès qui ont été définis en entrée ou en sortie. Dans ce cas toutes les centrales de l'installation passent en APB Global.

Si la fonction est désactivée sur une seule des centrales, elle sera automatiquement désactivée sur toutes les centrales de l'installation. Pour que l'anti-passback global fonctionne il est indispensable que le service SenatoFX.NET soit lancé et communique avec les centrales.

La fonction « Anti-Timeback » permet de réaliser un anti-passback en fonction d'une durée de temps à définir. Un même badge ne peut pas accéder 2 fois de suite sur un même accès, sans laisser s'écouler un certain temps, défini par le curseur Anti-Timeback. Ce temps peut être régler de 0 à 99 minutes. Lors que le temps est paramétré à 0, l'anti-timeback est désactivé, et c'est l'anti-passback qui fonctionne.

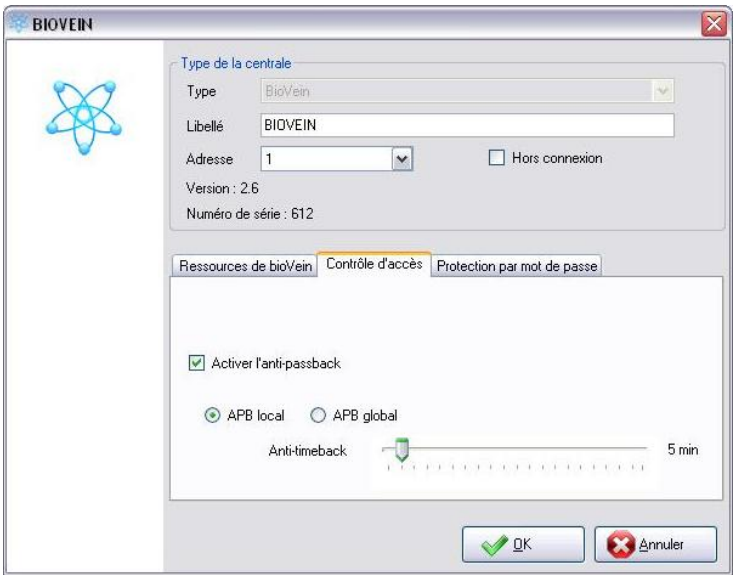
La fonction « Délai de transit » permet de limiter le temps dont les personnes disposent pour aller d'un accès à un autre. Au delà de ce temps, les utilisateurs sont refusés sur le second accès et sont contraints de retourner vers le premier.

Configuration du site

Paramétrage des centrales (suite)

1. Création d'une centrale (suite)

Descriptions de l'onglet « Contrôle d'accès » pour BIOVEIN



- Activez ou non « l'Anti-passback »
- Choisissez le mode « local » ou le mode « global »
- Activez ou non « l'Anti-timeback »
- Sélectionnez la durée de « l'Anti-timeback »

Validez par « OK » lorsque les réglages sont terminés.

Lorsque l'on active « l'anti-passback », les options « APB Local », « APB Global » et « Anti-timeback » apparaissent.

Pour que la fonction « Anti-passback » fonctionne sur le lecteur **BIOVEIN** en mode centrale, l'on ne peut utiliser que « l'Anti-Timeback » ou « l'APB Global » (Anti-Passback Global).

L' « APB Global » (Anti-Passback Global) permet d'activer la fonction anti-passback entre tous les accès du site qui ont été définis en entrée ou en sortie. Dans ce cas toutes les centrales de l'installation passent en APB Global. Si la fonction est désactivée sur une seule des centrales, elle sera automatiquement désactivée sur toutes les centrales de l'installation. Pour que l'anti-passback global fonctionne il est indispensable que le service SenatoFX.NET soit lancé et communique avec les centrales.

La fonction « Anti-Timeback » permet de réalisé un anti-passback en fonction d'une durée de temps à définir.
Un même identifiant ne peut pas accéder 2 fois de suite sur un même accès, sans laisser s'écouler un certain temps, défini par le curseur Anti-Timeback. Ce temps peut être régler de 0 à 99 minutes. Lors que le temps est paramétré à 0, l'anti-Timeback est désactivé, et c'est l'anti-passback qui fonctionne.

Le lecteur **BIOVEIN** peut être utilisé aussi en mode lecteur (voir page 44)

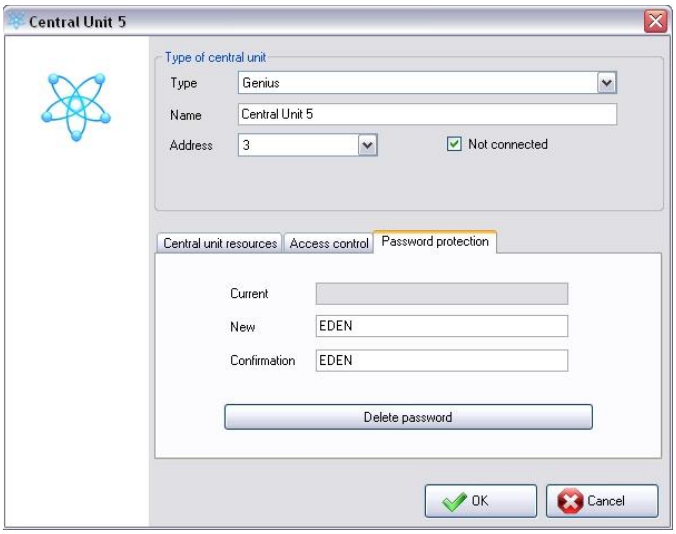
Configuration du site

Paramétrage des centrales (suite)

1. Création d'une centrale (suite)

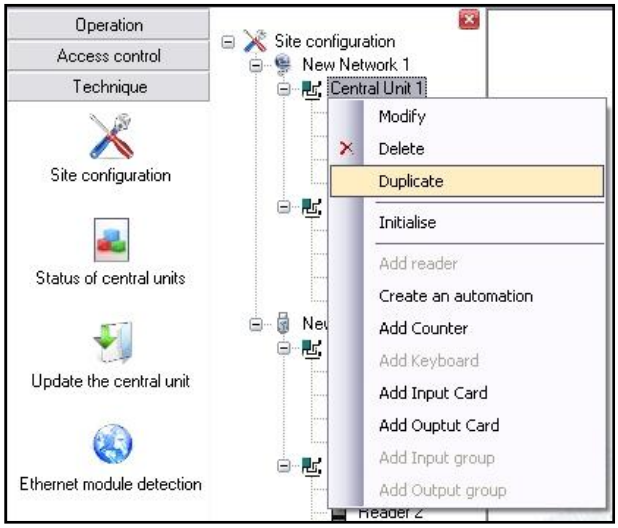
La protection par mot de passe permet lorsqu'un mot de passe est défini sur la centrale, d'empêcher la lecture, l'écriture ou l'effacement des données sur celle-ci.

Dans le cas ou une personne essaierait de se connecter à la centrale sans le mot de passe, la centrale passe dans le statut « Mot de passe incorrect » dans SenatorFX.NET.

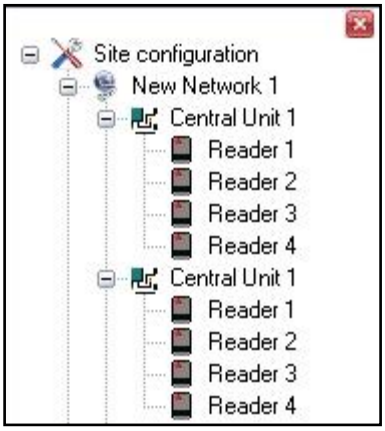


- Éditez le nouveau mot de passe de la centrale
- Confirmez le nouveau mot de passe de la centrale
- Si nécessaire supprimez le mot de passe de la centrale

1. Dupliquer une centrale



2. Sélectionnez la centrale à dupliquer et cliquez sur « Dupliquer »



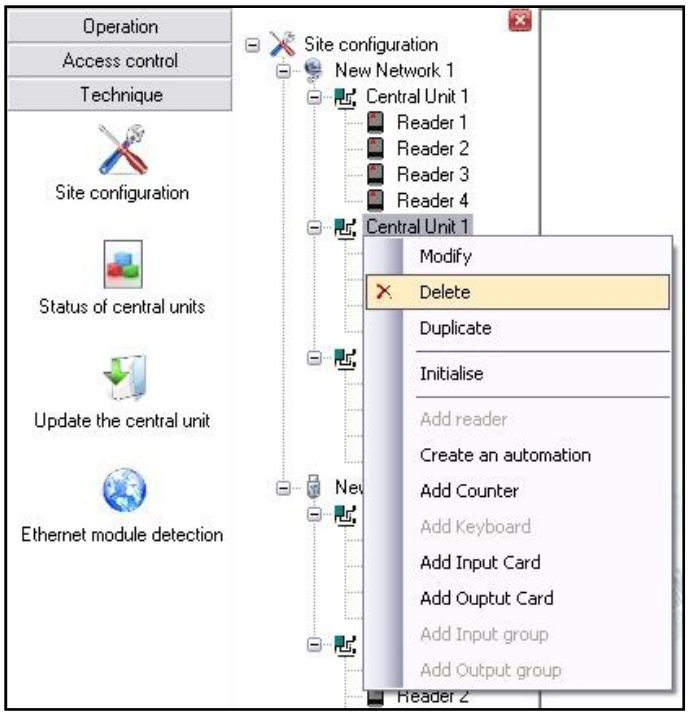
Le logiciel duplique totalement la centrale comprenant

- Les périphériques associés
- Le paramétrage
- Incrémentation de l'adresse disponible

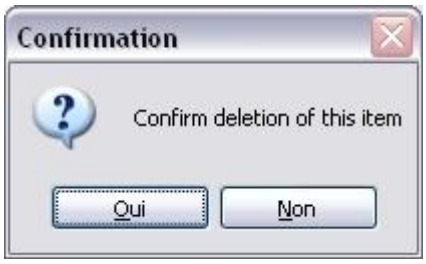
Configuration du site

Paramétrage des centrales (suite)

3. Supprimer une centrale



1. Sélectionnez la centrale à supprimer et cliquez sur « Supprimer »



2. Confirmez la suppression de la centrale

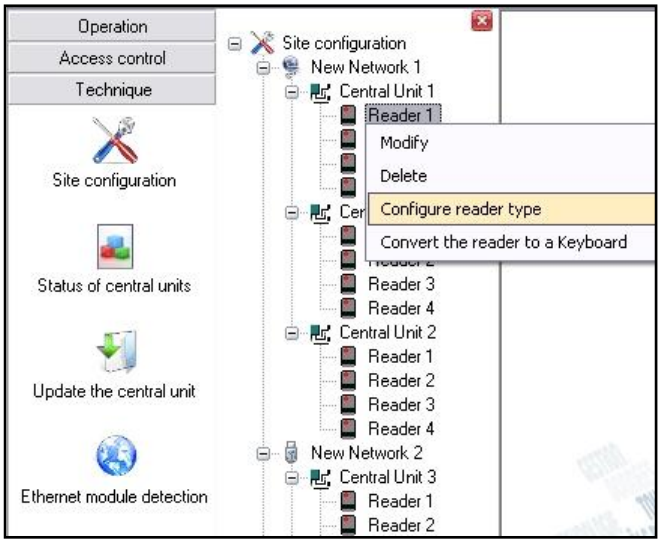
Nota: La suppression du réseau entrainera la suppression de tous les périphériques associés

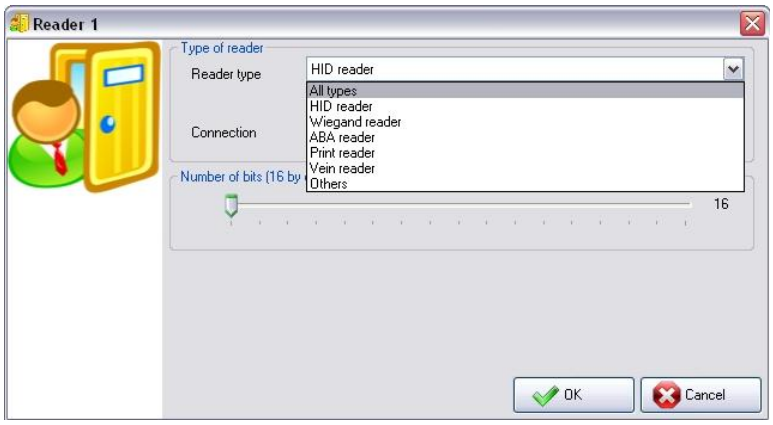
Configuration du site

Paramétrage des lecteurs

Sélectionnez le menu Technique → Configuration du site

1. Configurer le type de lecteur





Sélectionnez le lecteur à configurer ; puis cliquez sur « Configurer »

Technologie/Protocole	Description
HID	Lecture d'un badge jusqu'à 32 bits
HID Décimal	Lecture d'un badge jusqu'à 32 bits en décimal
Wiegand personnalisé	Config. avec code site, distributeur, parité paire/Impaire…
Wiegand décimal personnalisé	Config. avec code site, distributeur, parité paire/Impaire pour encodage des badges en décimal
Wiegand 26 bits	Lecture d'un badge jusqu'à 26 bits en Wiegand standard
Wiegand 27 bits	Lecture d'un badge jusqu'à 27 bits en Wiegand standard
Wiegand 30 bits	Lecture d'un badge jusqu'à 30 bits en Wiegand standard
BIOVEIN	Lecteur d'analyse du réseau veineux du doigt EDEN
INT-NPP	Lecteur pour reconnaissance de plaques d'immatriculation
ARGINA	Lecteur de badge proximité protégé par mot de passe EDEN
SOLO3000	Lecteur d'empreinte digitale EDEN capteur SAGEM (3000 Users)

Configuration du site

Paramétrage des lecteurs (suite)

1. Configurer le type de lecteur (suite)

Technologie/Protocole	Description
RK40	Lecteur ICLASS HID avec clavier intégré
ABA	Lecture d'un badge au format Clock/data sur 8 caractères
ABA personnalisé	Config. avec code site, distributeur, parité paire/Impaire…

Ce menu permet de configurer la technologie du lecteur raccordé à la centrale.

Le champ type de lecteur indique et permet de choisir le type de lecteur raccordé à la centrale.

Le tableau présente les différents choix possibles.

- **En mode Wiegand les centrales EDEN peuvent lire un N° de badge sur 32 bits.**
- **En mode Clock/data les centrales EDEN peuvent lire un N° de badge sur 8 caractères.**

Répétez cette action pour chaque lecteur des centrales de gestion locale de l'installation.

Configuration du site

Paramétrage des lecteurs (suite)

Sélectionnez le menu Technique → Configuration du site

1. Configurer le type de lecteur (suite)

Description des formats personnalisés:

Wiegand personnalisé, Wiegand Décimal personnalisé, ABA personnalisé

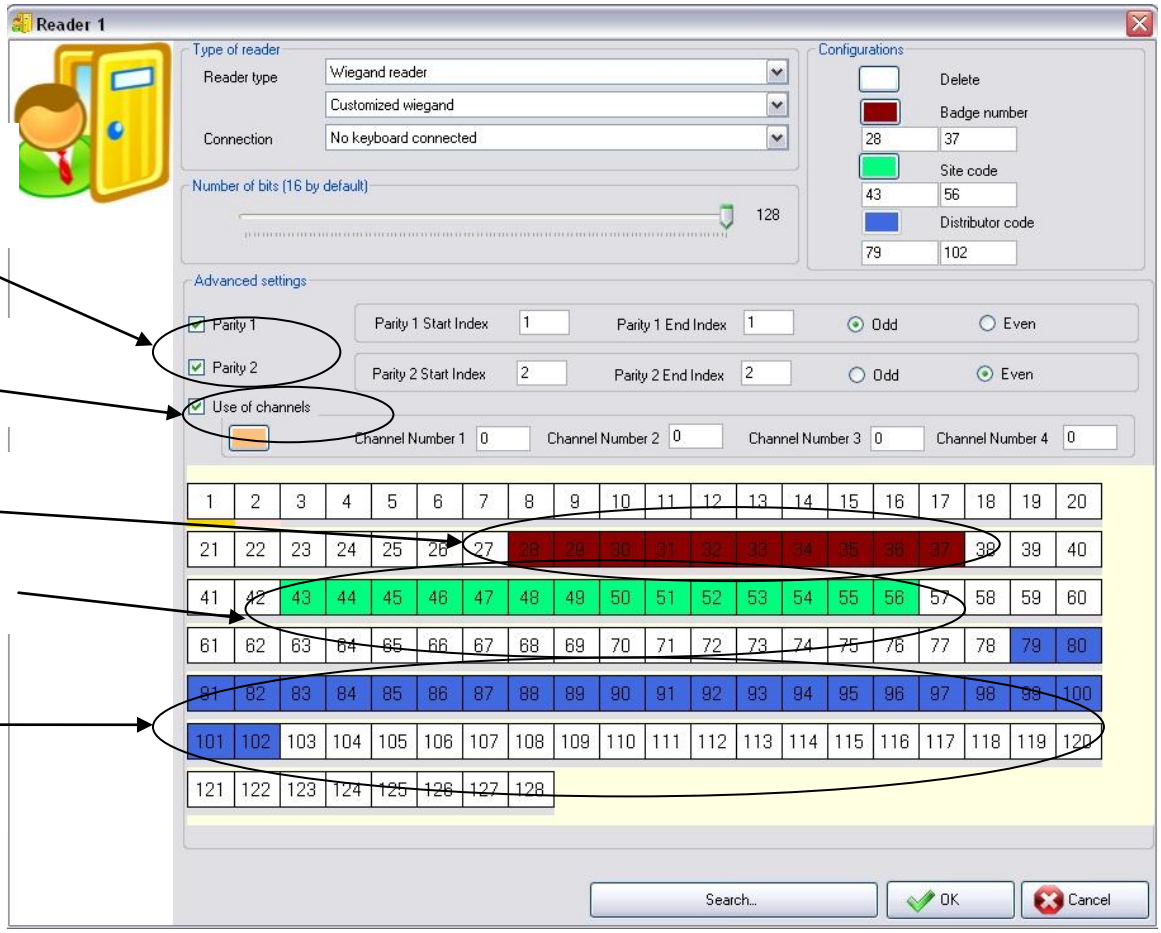
Gestion des parités avec index de début/fin

Paramétrage des canaux 1,2, 3 et 4

Positionnement du code du badge

Positionnement du code site

Positionnement du code distributeur



Rappel

Dans tous les modes « Wiegand » les centrales EDEN savent lire l'encodage du N° d'un badge jusqu'à 32 bits.

Dans tous les modes « ABA » les centrales EDEN savent lire l'encodage du N° d'un badge jusqu'à 8 caractères.

Les centrales de gestion local EDEN acceptent un format de lecteur différent par entrée « lecteur » soit

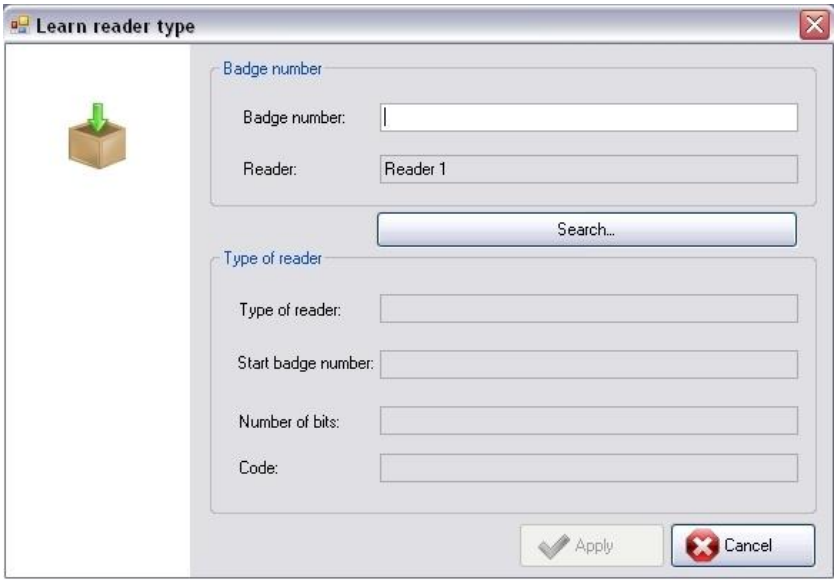
- **GENIUS** / **C1P2FX** = 2 lecteurs = 2 formats de lecteurs différents
- **C4PLUSFX** = 4 lecteurs = 4 formats de lecteurs différents

Configuration du site

Paramétrage des lecteurs (suite)

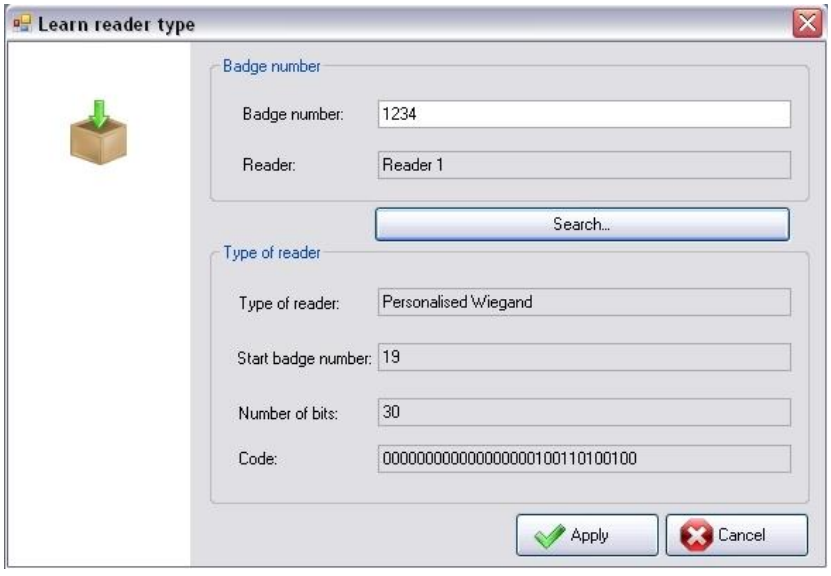
2. Détection automatique du format de badges existant

Lors de la récupération de badges existant sur un site, le logiciel **SENATORFX.NET** permet une détection automatique du format d'encodage des badges via un des lecteurs de l'installation.



Procédure :

- Choisissez un lecteur d'une centrale déjà connectée et fonctionnelle
- Entrez le numéro du badge à reconnaître
- Cliquez sur le bouton "Recherche..."
- Passez ensuite le badge devant le lecteur



Résultat :

SenatorFX.NET affiche le type de lecteur, le numéro de badge, le nombre de bits et le code.
Il vous suffit ensuite de cliquer sur "Appliquer" pour que la configuration soit automatiquement appliquée au lecteur.

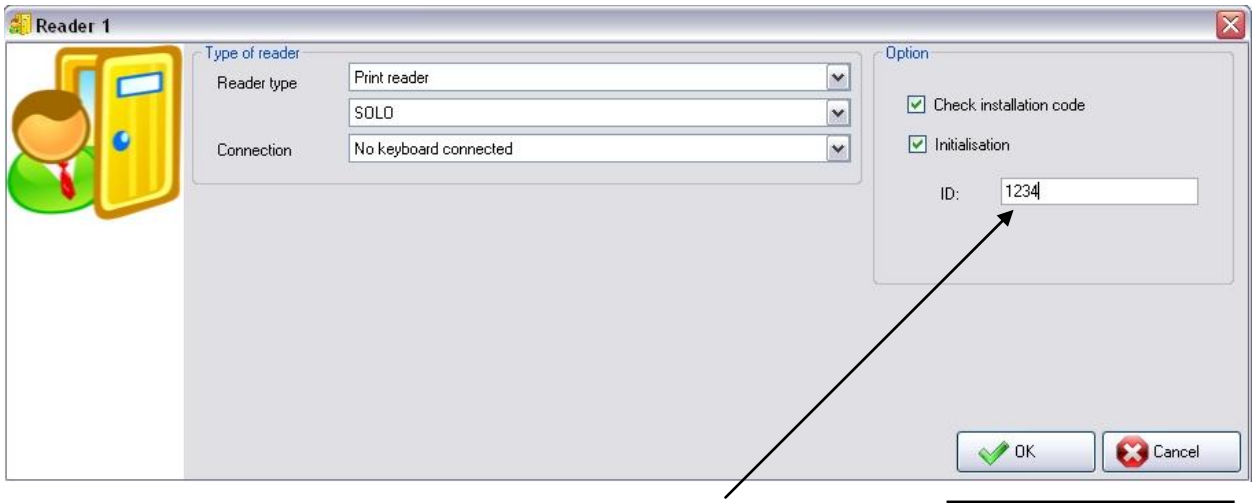
Configuration du site

Paramétrage des lecteurs (suite)

3. La biométrie

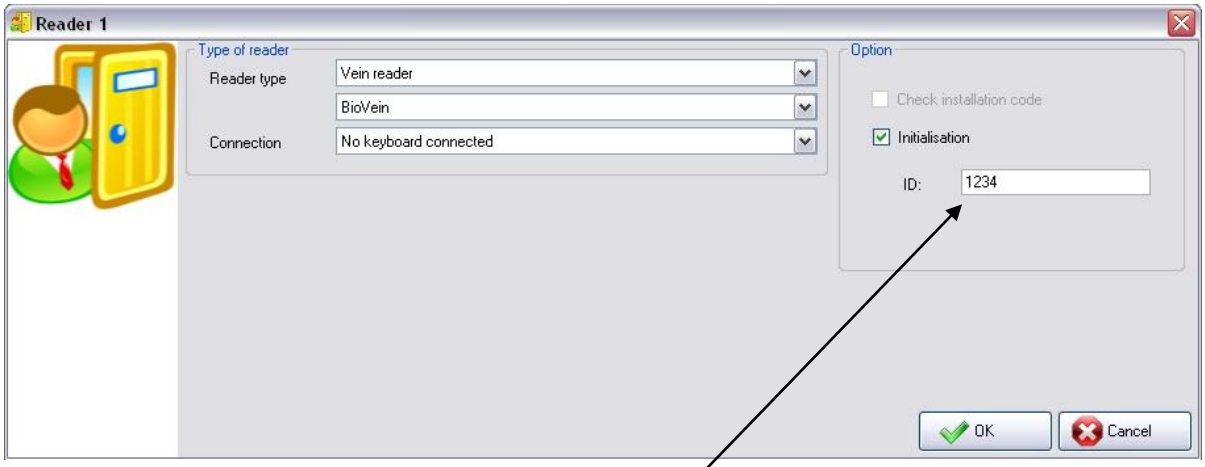
SenatorFX.NET offre la possibilité d'utiliser la biométrie sur votre installation les lecteurs, SOLO/SOLO3000 (capteurs optiques) ou BIOVEIN (réseau veineux).

Lecteurs d'empreintes digitales, SOLO/SOLO3000



Saisissez l'identifiant du lecteur édité sur l'étiquette collée dans le lecteur

Lecteur de reconnaissance du réseau veineux du doigt **BIOVEIN**



Saisissez l'identifiant du lecteur édité dans le menu information du lecteur BIOVEIN.

Si les lecteurs biométriques EDEN sont connectés aux centrales via un Bus RS485 et non sur les bornes « lecteur », ils **prennent la place d'un lecteur pour la centrale aussi.**

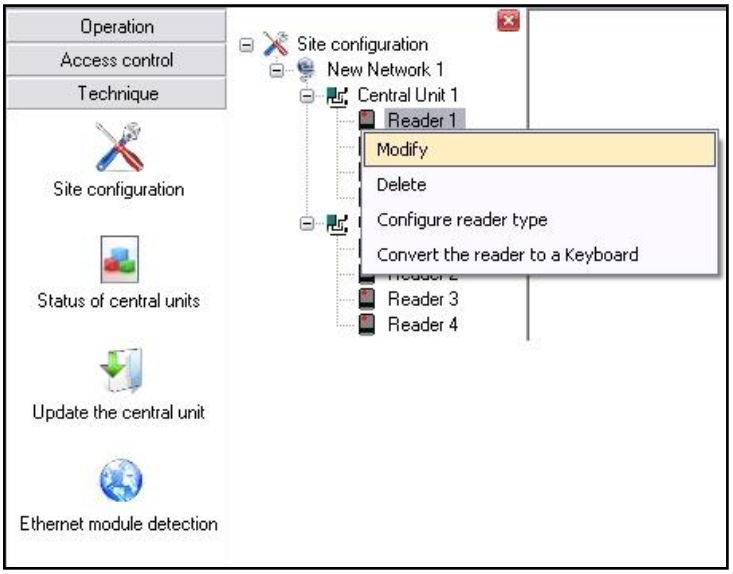
GENIUS/C1P2FX = 2 lecteurs **C4PLUSFX** = 4 lecteurs

Configuration du site

Paramétrage des lecteurs (suite)

4. Paramétrer un lecteur

Ce menu permet de régler tous les paramètres associés aux lecteurs



1. Sélectionnez le lecteur à paramétrer et cliquez sur « modifier »

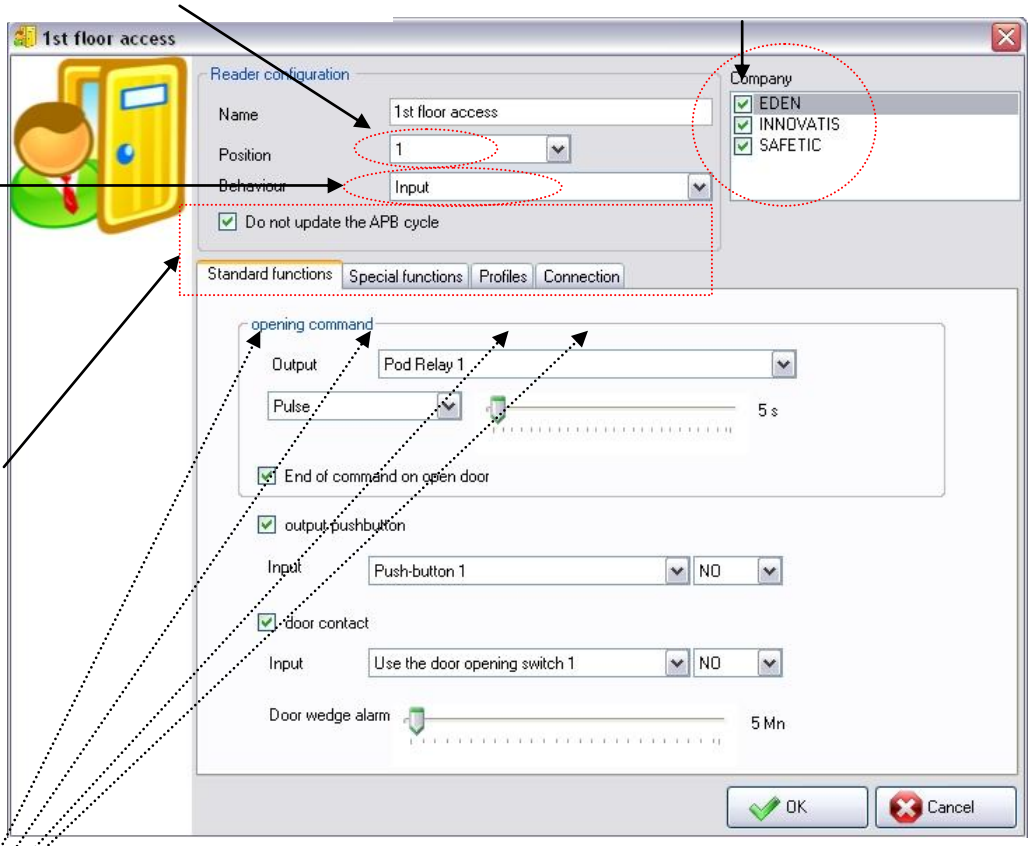
Le champ « Société » permet de définir à quelle société appartient l'élément. Certains éléments peuvent appartenir à plusieurs sociétés, comme pour un lecteur d'entrée commune par exemple.

Le champ « Libellé » permet d'éditer le nom du lecteur qui s'affichera dans le logiciel.

Le menu « Position » indique l'entrée sur laquelle le lecteur se trouve sur la centrale.

Le menu « Comportement » indique l'utilisation qui est fait de la porte. Les comportements disponibles sont « Neutre », « Entrée », « Sortie ». L'information du comportement est dédiée pour la fonction Anti-Passback et la définition de zones.

L'option « ne pas mettre à jour le cycle APB », lorsqu'elle est cochée, autorise les gens qui passent sur le lecteur à ne pas changer leur statut Anti-Passback.



Certains onglets diffèrent suivant le type de lecteur déclaré et raccordé

Configuration du site

Paramétrage des lecteurs (suite)

5. Onglet « Fonctions standards »

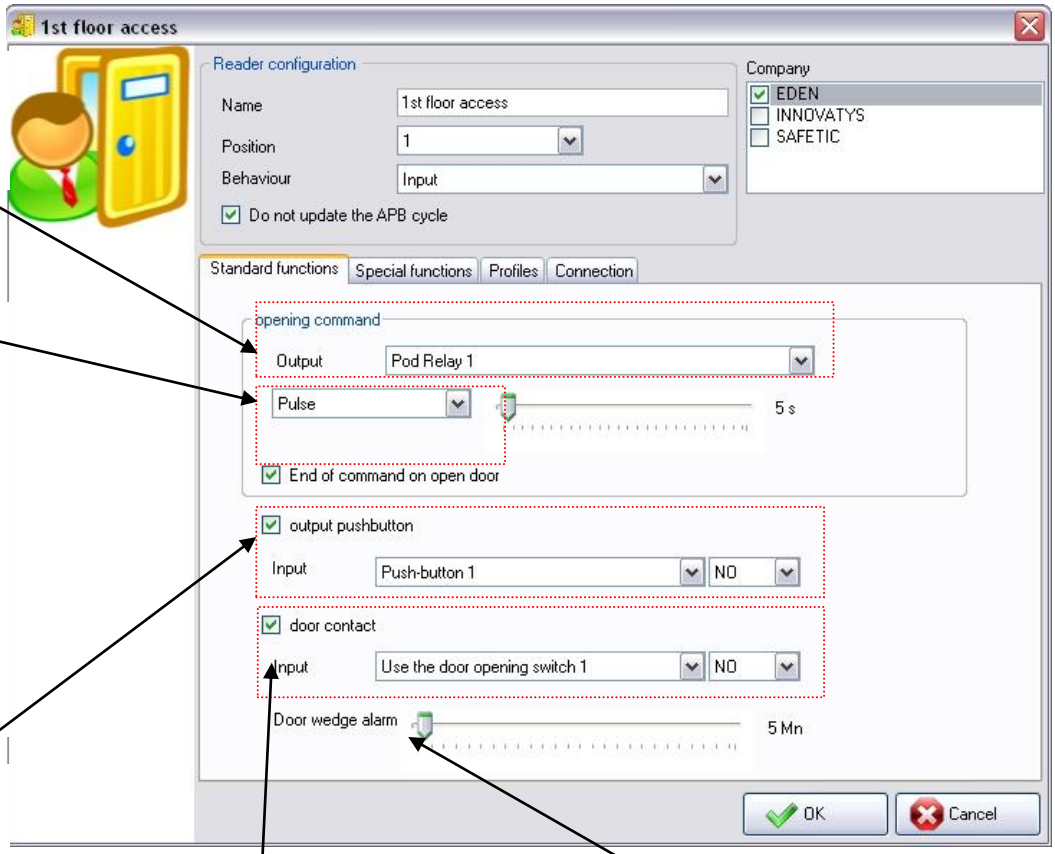
Description des paramètres de contrôle d'accès basiques liés aux lecteurs

Le champ « Sortie », défini la sortie qui sera activée au passage d'un badge autorisé sur le lecteur.

Ce champ indique le mode de commutation du relais. Les choix sont « Impulsion » et « Alternée».

Le mode impulsion est réglable de 1 à 255 secondes, à l'aide du curseur.

L'option « Fin de commande sur porte ouverte », lorsqu'elle est cochée, désactive le relais d'ouverture dès lors que la porte est ouverte.



Si vous utilisez un bouton de sortie, cochez cette case.

Choisissez l'entrée de la centrale souhaitée et son mode de fonctionnement, NO ou NF.

Cochez cette case si vous souhaitez gérer l'état de la porte contrôlée

Choisir l'entrée de la centrale souhaitée et son mode de fonctionnement, NO ou NF.

Cela permettra de gérer l'alarme « porte forcée ».

« Alarme blocage » permet de gérer et paramétrer l'alarme porte trop longtemps ouverte » qui se déclenche, si la porte reste bloquée ouverte plus longtemps que le délai autorisé programmé.

Le compteur est paramétrable de 0 à 255 minutes.

Lorsque le compteur est à 0, l'alarme est désactivée.

Configuration du site

Paramétrage des lecteurs (suite)

6. Onglet « Fonctions spéciales »

Description des paramètres auxiliaires liés aux lecteurs

Cochez la case de l'option « entrée sous condition » si vous souhaitez déclencher l'autorisation d'accès seulement aux véhicules détectés par un système tiers, telle une boucle au sol.

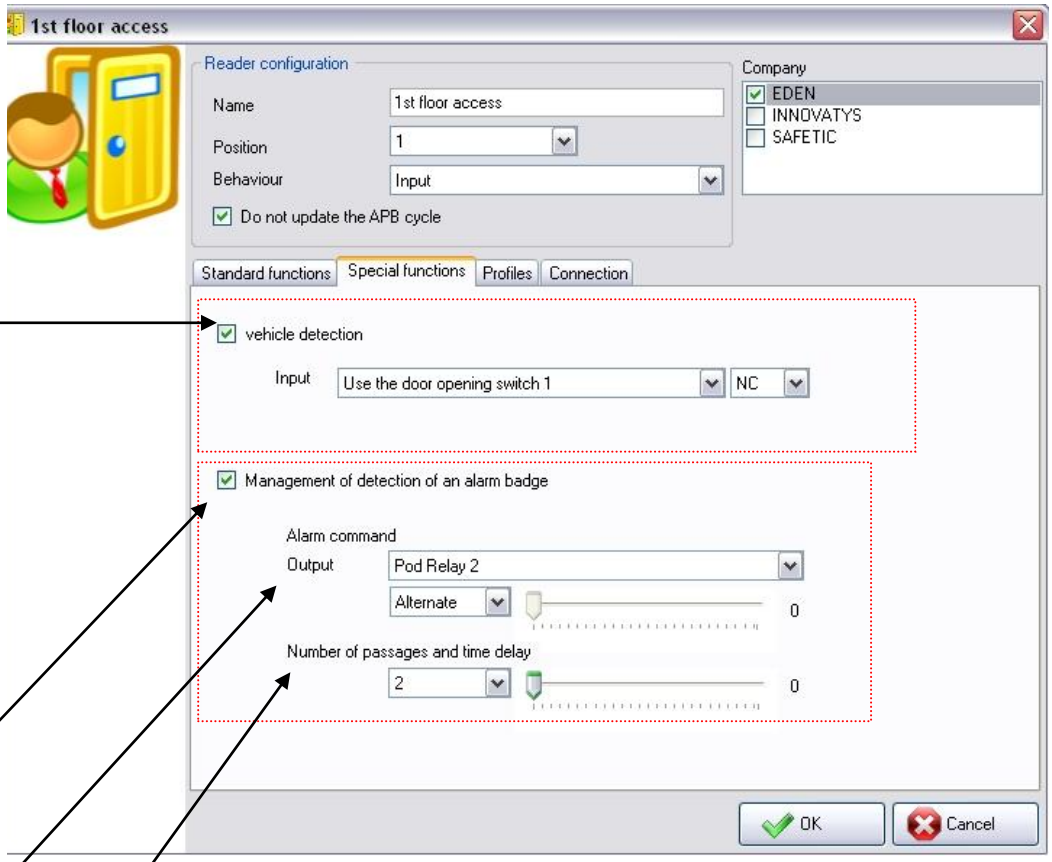
Sélectionnez l'entrée et son mode « NO ou NF » ou sera raccordé le système de détection de véhicule.

Si un badge est présenté au lecteur sans détection de véhicule, l'accès sera refusé avec l'information « Véhicule non détecté ».

Validation de la fonction « Badge Alarme »

Choix de la sortie relais de la centrale et de son mode.

Programmez le nombre de passages nécessaires des « Badges Alarme » et du délai de cette action.



La détection d'un « **Badge Alarme** » permet de déclencher une sortie supplémentaire à celle de la porte pour une action tierce.

Les conditions

- Le badge doit avoir le statut « badge Alarme »
- Le lecteur doit avoir la fonction « badge Alarme » validée
- Le badge doit être autorisé sur le lecteur
- Nombre de passage du badge acceptés dans le temps prescrit (minimum 2 passages)

L'action

- Activez une sortie relais de la centrale en mode temporisée de 1 à 255 secondes ou alternée.

Différence pour le Biovein

- Le doigt Alarme est le 2ème doigt enregistré
- Un seul passage du doigt déclenche la sortie relais

Configuration du site

Paramétrage des lecteurs (suite)

7. Onglet « Profils »

Description des paramètres auxiliaires liés aux lecteurs

La zone « Profils » contient trois onglets:

Niveaux d'alerte 0, 1 et 2.

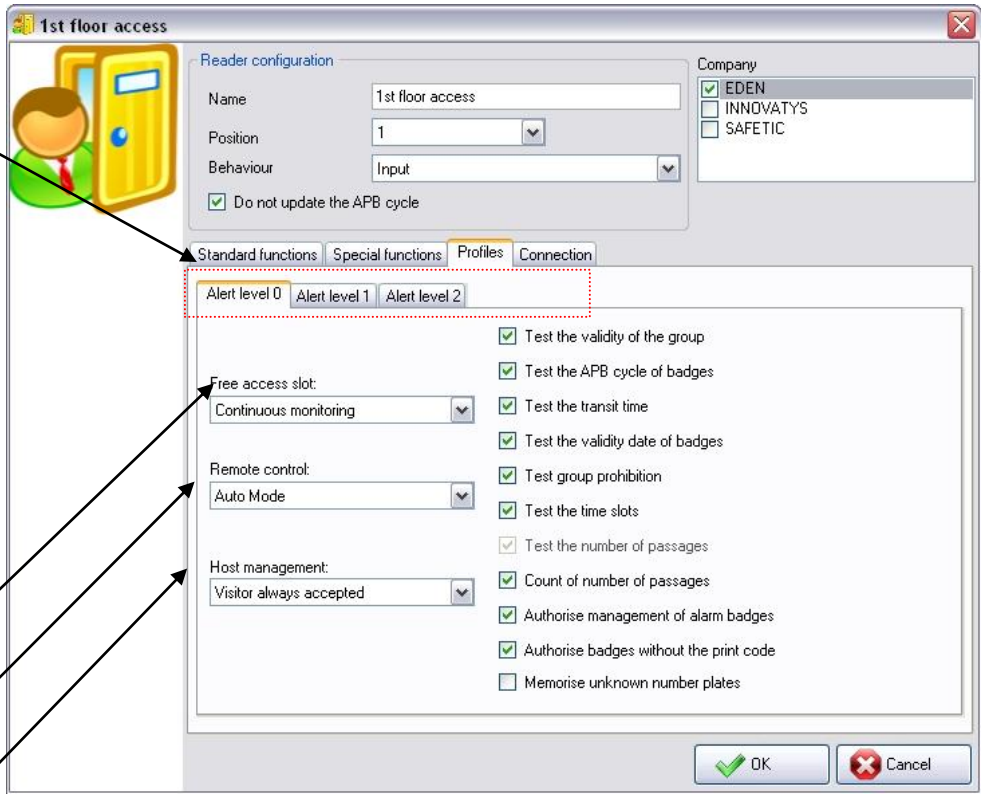
Chaque onglet intègre les mêmes paramètres qui seront activés via la gestion d'état de crise managée par les opérateurs du logiciel ou via des « automatismes » préétablis.

Les différents profils de gestion d'états de crise ne peuvent être activés en même temps.

L'indication du niveau d'alerte en cours, est toujours visible dans le logiciel, dans la barre d'informations en bas de la fenêtre de SenatorFX.NET.

Plage d'accès libre permet d'affecter des plages horaires pendant lesquelles l'accès est déverrouillé (page 55).

Télécommande permet de définir le mode dans lequel se trouve l'accès.



Gestion accompagnateur : indique la manière dont les personnes accompagnées sont gérées.

Les choix sont :

Accompagné + accompagnateur,
Accompagné toujours refusé,
Accompagné toujours accepté.

Si les cases sont cochées ☑

Tester la validité du groupe = Si groupe d'accès valide alors accès autorisé

Tester le cycle APB du badge = Si statut APB du badge est valide alors accès autorisé

Tester le délai de transit = Si statut de délai de transit du badge est HS alors accès refusé

Tester la date de validité des badges = Si date de validité dépassée alors accès refusé

Tester interdiction des groupes = Si groupe est interdit alors accès refusé

Tester les plages horaires = Vérification du statut de la plage horaire du badge

Tester le nombre de passage = Vérifier que le badge possède encore un crédit de passage

Décompte du NB de passages = Si badge avec crédit de passage alors décompte à chaque passage sur ce lecteur d'un crédit d'une unité de passage.

Autoriser la gestion des « Badges Alarme » = Active la fonction décrite page 37

Autoriser les badges sans code/empreinte = Autoriser l'accès à des badges configurés en badge seul sans code ni empreinte, pour les systèmes à badge+empreintes et badge+code.

Mémoriser les plaques inconnues = Mémoriser les plaques d'immatriculation non enregistrées dans le système via le lecteur dédié à cette application INTNPP.

Configuration du site

Paramétrage des lecteurs (suite)

8. Onglet « Raccordements »

Description des paramètres auxiliaires liés aux lecteurs

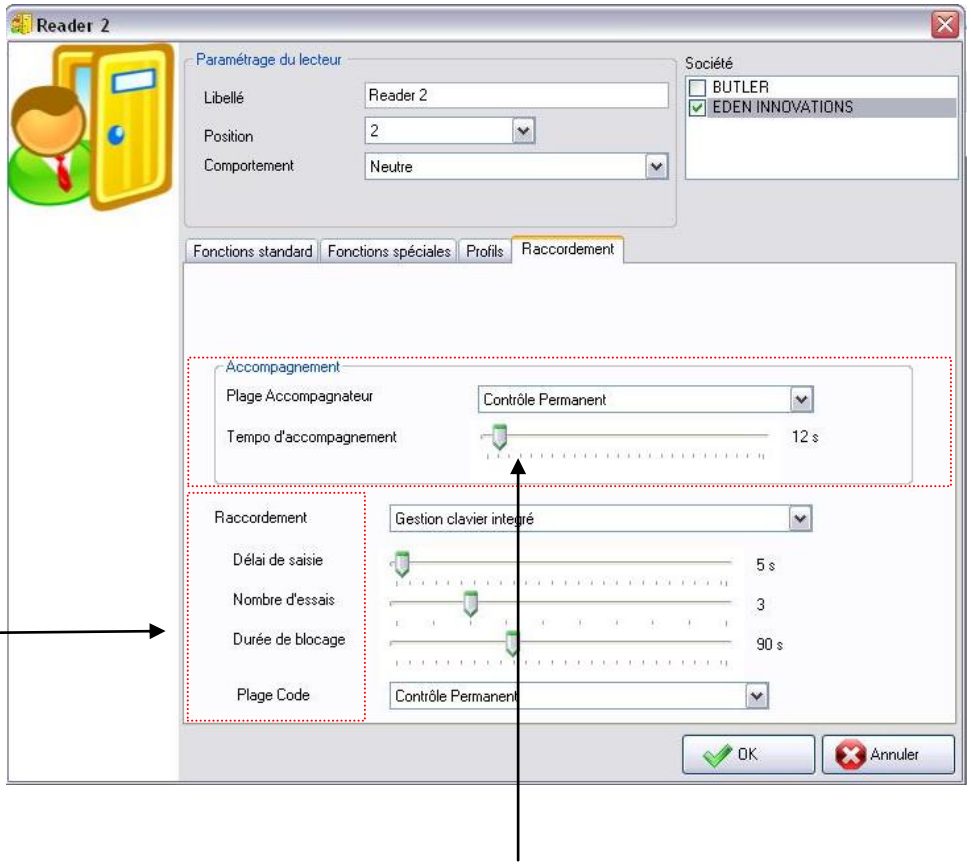
« Gestion clavier intégré »

Permet d'utiliser un lecteur avec clavier intégré, et de déclencher une double identification.

Le « Délai de saisie » permet de paramétrer le temps dont dispose l'utilisateur pour taper son code après présentation de son badge. Le « Nombre d'essais » indique le nombre de mauvais code qui peuvent être tapés avant le blocage du clavier. La « Durée de blocage » définie la durée pendant laquelle le clavier est bloqué après saisies de mauvais codes.

La « Plage code » permet de définir des plages horaires durant lesquelles le code n'est pas demandé.

Pour définir une plage, il faut une plage automatisme (**menu Contrôle d'accès**).



« **Accompagnement** » permet de définir les paramètres liés à la fonction accompagnateur/accompagné.
Le champ « Plage accompagnateur » permet de définir des plages durant lesquelles l'accompagnateur doit obligatoirement être avec l'accompagné.

Durant ces périodes, l'accompagné présente son badge, et, pour débloqué l'accès, l'accompagnateur dispose d'un temps paramétrable pour présenter le sien.

Pour cette fonction, il faut créer une plage automatisme (**menu Contrôle d'accès**).

En dehors de ces plages, « l'accompagné », peut se déplacer librement sur les accès.

La « Tempo d'accompagnement » permet de définir le temps dont dispose l'accompagnateur pour présenter son badge, après le passage du badge accompagné.

Configuration du site

Paramétrage des lecteurs (suite)

9. Onglet « Caractéristiques »

Description des paramètres auxiliaires liés aux lecteurs biométriques, **SOLO**/**SOLO3000** et **BIOVEIN**

Réglage du capteur du lecteur

Nombre d'enrôlements
Défini le nombre de passage du doigt de l'utilisateur pour être enrôlé.
Réglage entre 3 et 5 passages

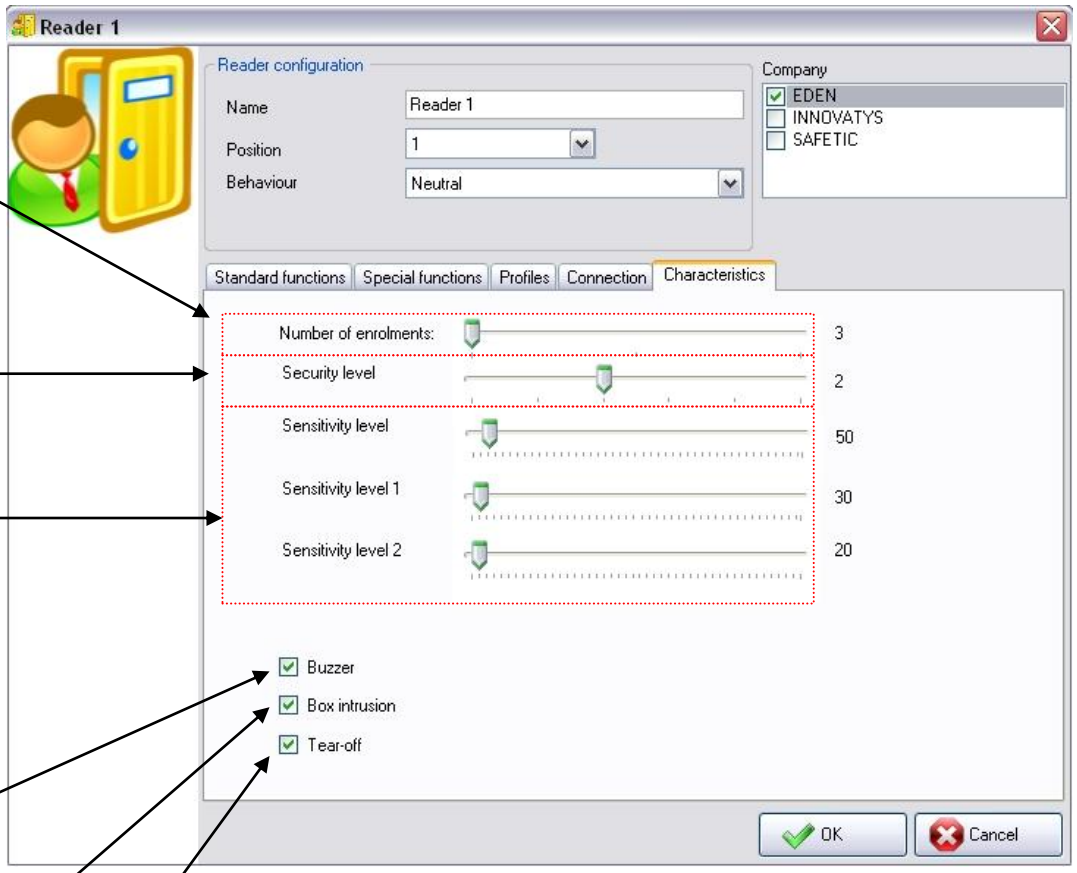
Niveau de sécurité
Réglable de 0 à 5 (défaut = 2)

Sensibilité
De 8 à 900 (50 par défaut)
Sensibilité 1
De 8 à 900 (30 par défaut)
Sensibilité 2
De 0 à 900 (20 par défaut)

Buzzer
Si la case est cochée alors le buzzer du lecteur activé

Effraction boîtier
Si case cochée alors gestion de l'effraction à l'ouverture du boîtier activée.

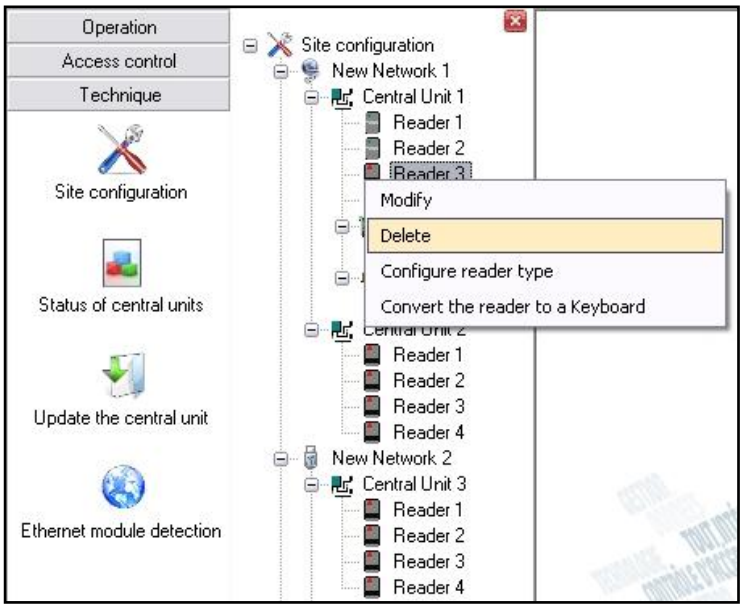
Arrachement
Si la case est cochée alors la gestion de l'effraction à l'arrachement du boîtier est activée.

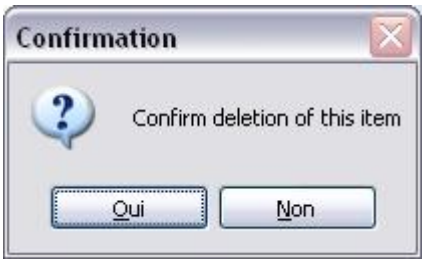


Configuration du site

Paramétrage des lecteurs (suite)

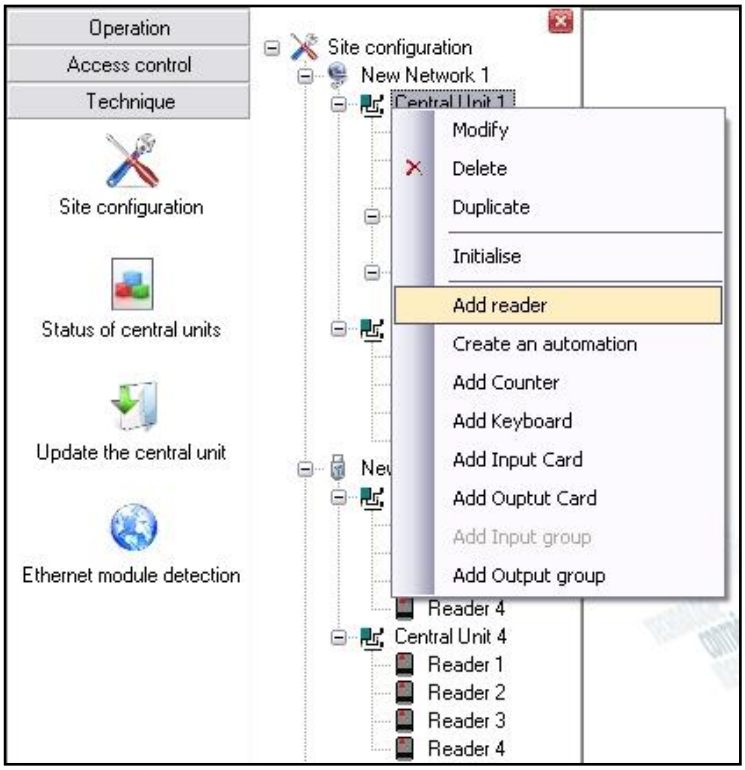
10. Supprimer/rajouter un lecteur





La suppression du lecteur fiche entrainera la suppression de tout le paramétrage associé

Pour ajouter un lecteur en lieu et place de ceux « supprimés » précédemment



Procédure :

1.Sélectionnez la centrale
2.Cliquez sur « ajouter lecteur »
3.Suivez les instructions pour paramétrer la fiche du lecteur (page 40)

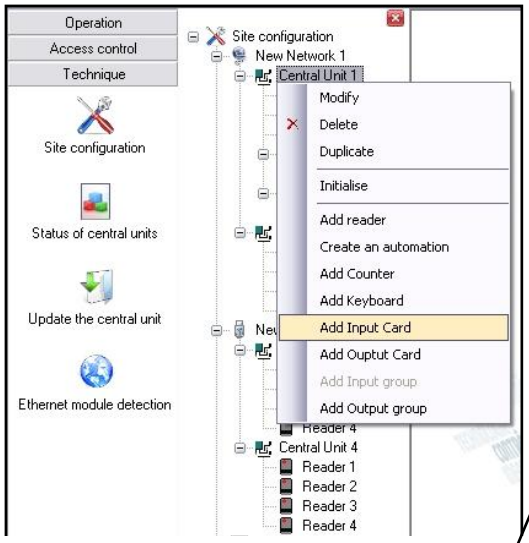
Configuration du site

Les périphériques des centrales

Sélectionnez le menu Technique → Configuration du site → Ajouter carte entrées

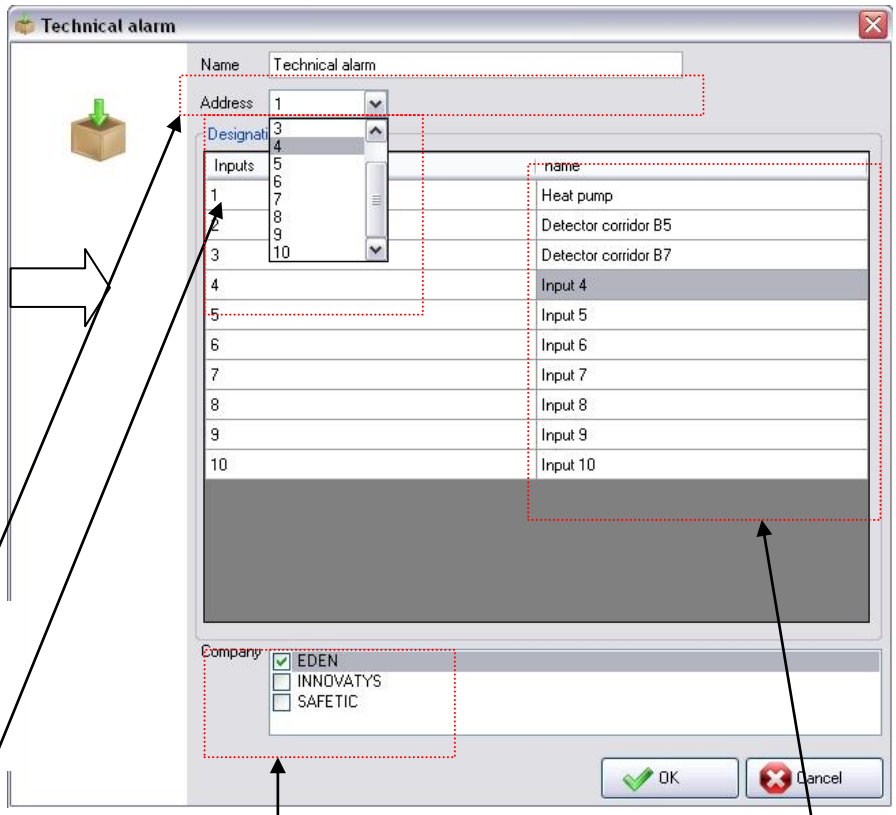
1. Les modules d'extension d'entrées

Ajouter une carte d'entrées



1. Sélectionnez la centrale

Cliquez puis sélectionnez :« Ajouter carte d'entrées »



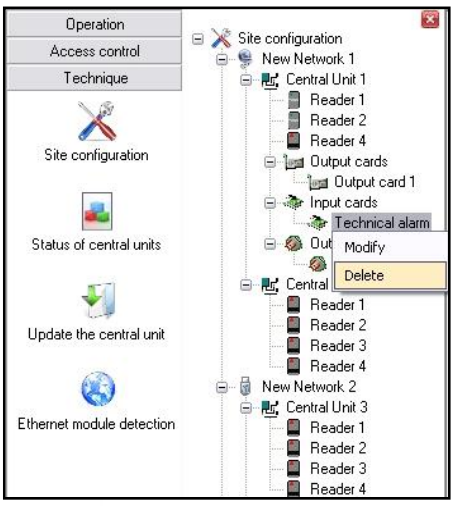
Le champ « **Libellé** » permet de définir le nom que portera la carte dans le logiciel.

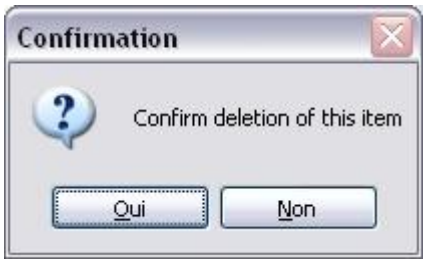
Le menu déroulant « **Adresse** » permet d'indiquer l'adresse qui a été définie sur la carte (1 à 10).

Le champ « **Société** » permet de définir à quelle société appartient l'élément. Certains éléments peuvent appartenir à plusieurs sociétés ou locataires.

Vous pouvez éditer un nom pour chaque entrée dans la liste « Libellé ».

Supprimer une carte d'entrées





Confirmez la suppression du groupe d'entrées

Note : La suppression d'une carte d'entrées entrainera la suppression de tout le paramétrage associé

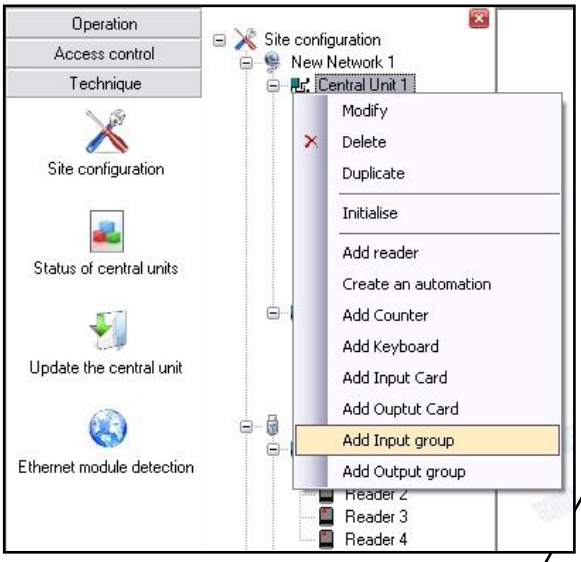
Configuration du site

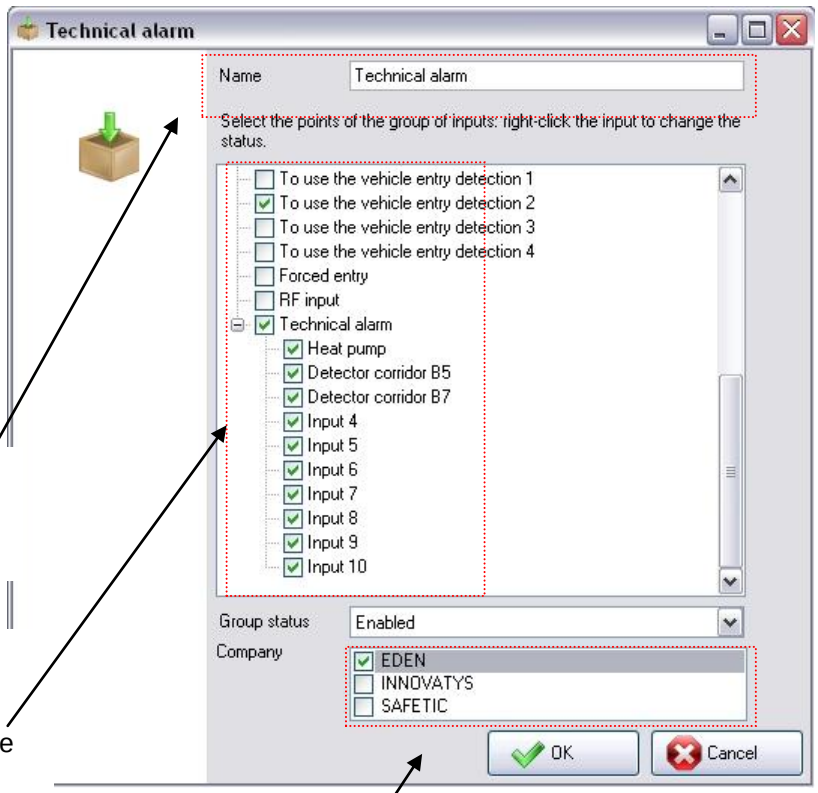
Les périphériques des centrales (suite)

2. Création des groupes d'entrées

Le groupe d'entrées est une association de plusieurs entrées d'une carte INFX2 et/ou d'entrées de la centrale.

Il peut être associé dans un « Automatisme » pour piloter différentes actions paramétrables.



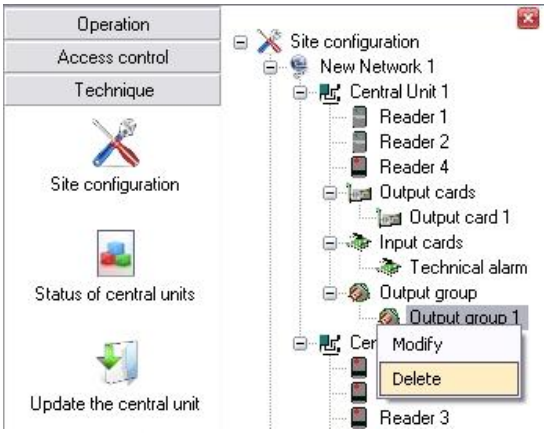


Le champ « Libellé » permet de définir l'appellation du groupe.

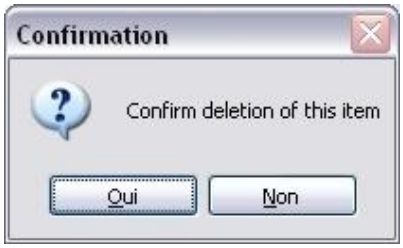
La liste « Sélectionner les entrées » permet de sélectionner les entrées qui feront parti du groupe.

Le champ « **Société** » permet de définir à quelle société appartient l'élément. Certains éléments peuvent appartenir à plusieurs sociétés.

Sélectionnez le Groupe d'Entrées et cliquez sur « Supprimer »



<u>Supprimer un Groupe d'Entrées</u>



Confirmez la suppression du groupe d'entrées

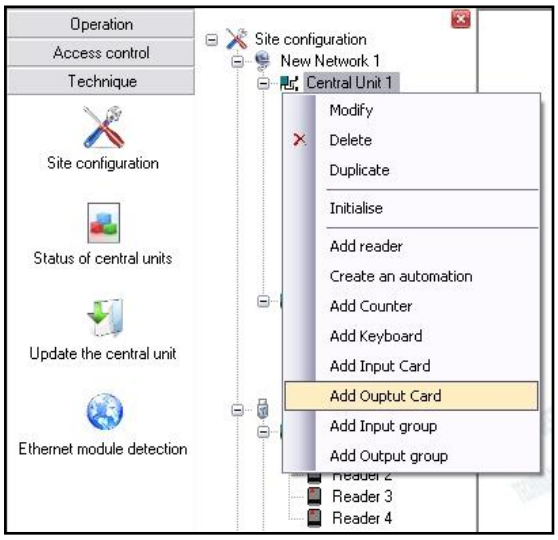
Nota: La suppression du groupe d'entrées entrainera la suppression de tout le paramétrage associé

Configuration du site

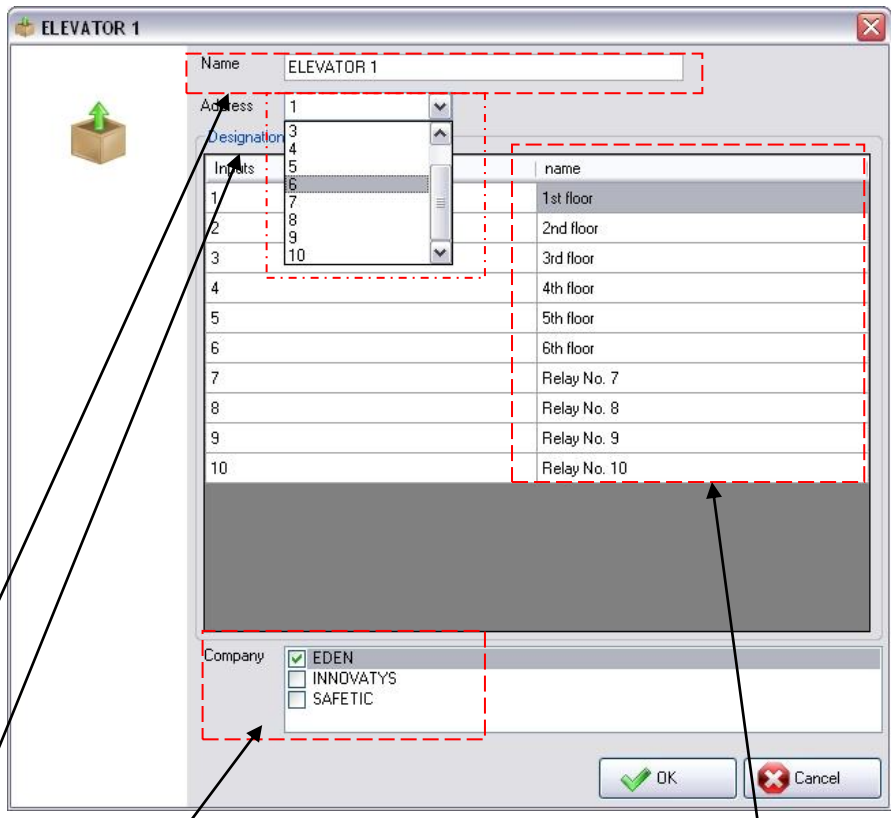
Les périphériques des centrales (suite)

3. Les modules d'extension de sorties

Ajouter une carte de sorties OUTFX2



- Sélectionnez la centrale
- Cliquez sur « Ajouter carte de sorties »



Le champ « **Libellé** » permet de définir le nom que portera la carte dans le logiciel

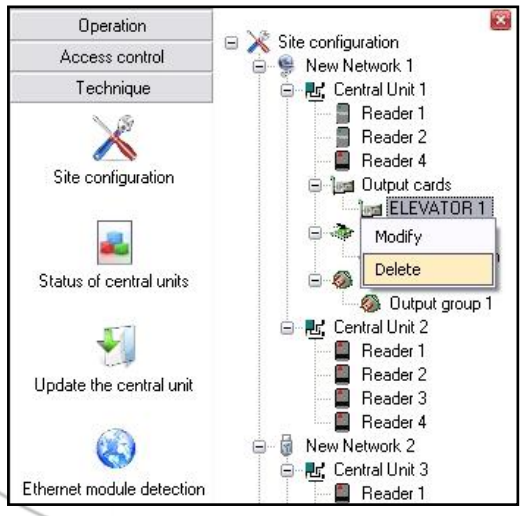
Le menu déroulant « **Adresse** » permet d'indiquer l'adresse qui a été défini sur la carte (1 à 10).

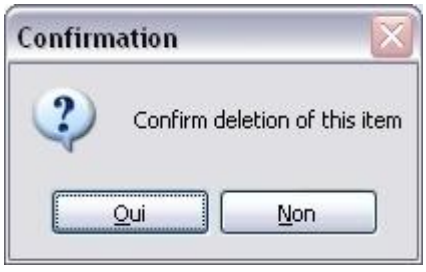
Le champ « **Société** » permet de définir à quelle société appartient l'élément. Certains éléments peuvent appartenir à plusieurs sociétés ou locataire.

Vous pouvez éditer un nom pour chaque entrée dans la liste « Libellé ».

Sélectionnez une carte de sortie et cliquez sur « Supprimer »

Supprimer une carte de Sorties





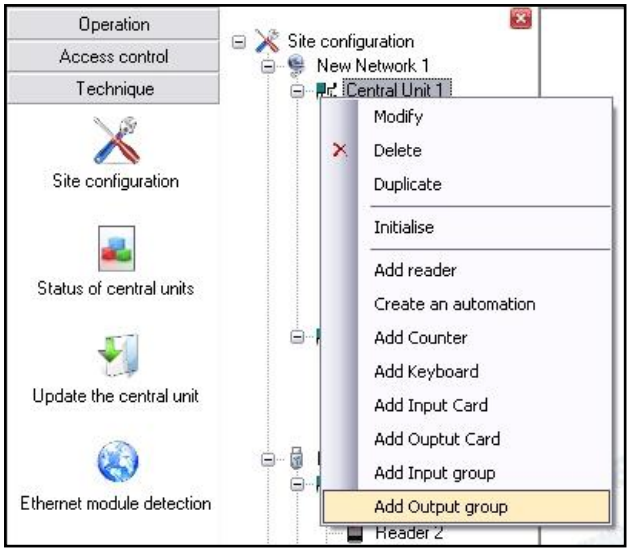
Confirmez la suppression du groupe d'entrées
La suppression du groupe d'entrées entrainera la suppression de tout le paramétrage associé

Configuration du site

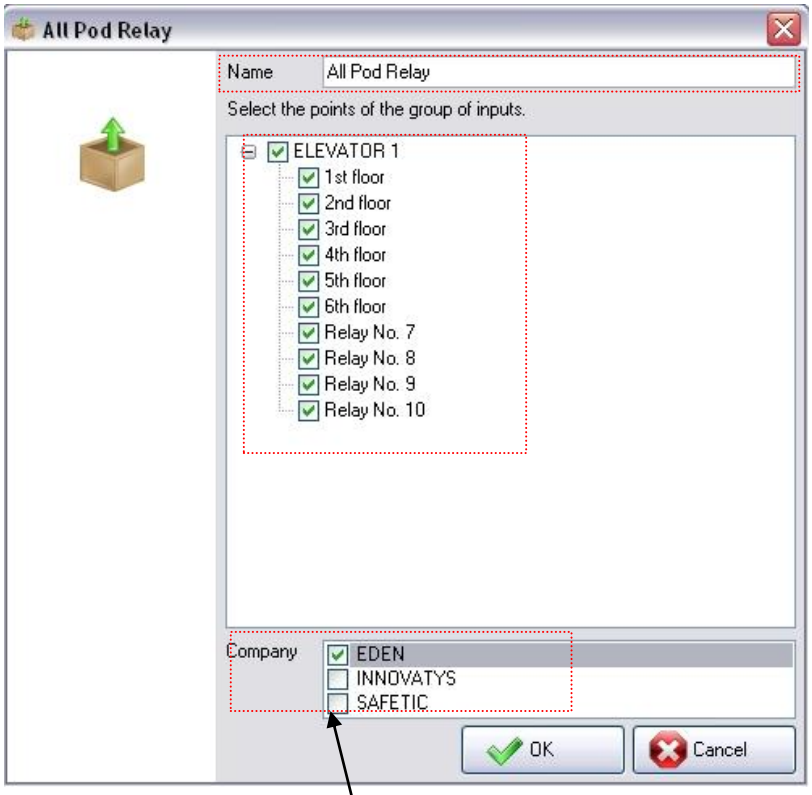
Les périphériques des centrales (suite)

4. Création des groupes de sorties

Le groupe de Sorties est une association de plusieurs sorties d'une carte **OUTFX2**.Il peut être associé dans un « Automatisme » comme action paramétrables, ou gestion d'ascenseur.



- Sélectionnez la centrale
- Cliquez sur « Ajouter groupe de sorties »

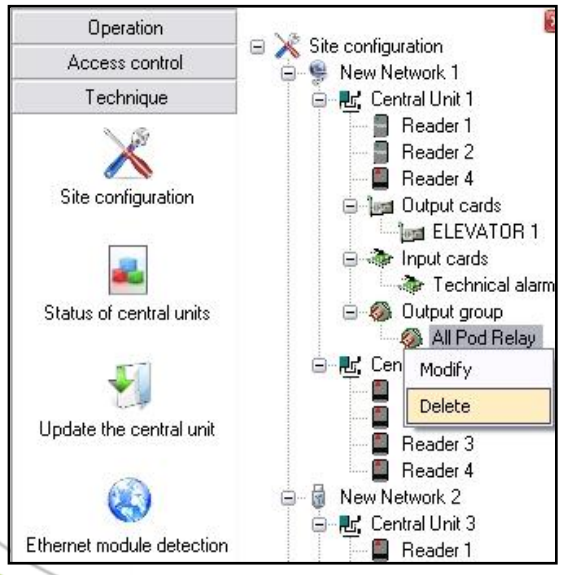


Le champ « **Libellé** » définit l'appellation du groupe

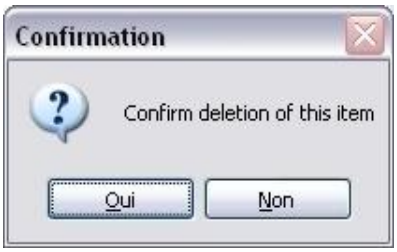
La liste « Sélectionner les Sorties » sert à sélectionner les entrées qui feront parti du groupe

Le champ « **Société** » permet de définir à quelle société appartient l'élément. Certains éléments peuvent appartenir à plusieurs sociétés ou locataire.

Sélectionnez le groupe de sortie et cliquez sur « Supprimer »



<u>Supprimer une groupe de sorties</u>



Confirmez la suppression du groupe d'entrées
La suppression du groupe d'entrées entrainera la suppression de tout le paramétrage associé

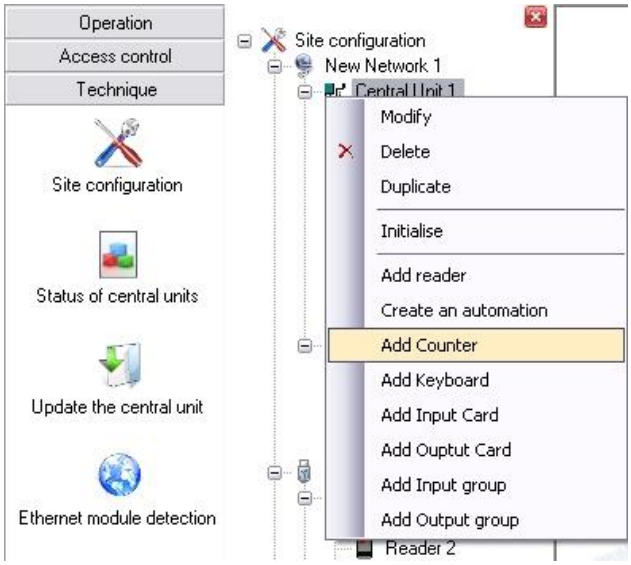
Configuration du site

Les périphériques des centrales (suite)

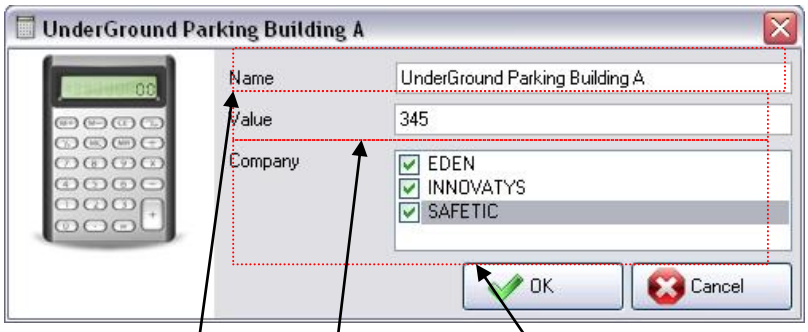
5. Les compteurs

Ils servent à connaître le nombre exact de personnes dans une zone, d'interdire l'accès lorsque le maximum de personnes autorisées est atteint pour une application de gestion de Parking ou pour des raisons de sécurité, de piloter un système tiers lorsqu'une zone est entièrement vide de tout usager.

Les compteurs peuvent à la fois servir de condition, être modifiés dans des automatismes et être affichés sur un plan dynamique de supervision.



Sélectionnez la centrale et cliquez sur « Ajouter Groupe de Sorties »

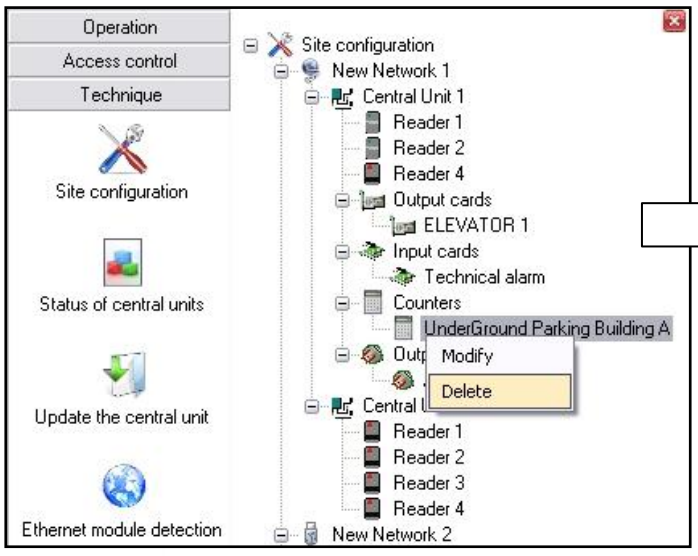


Le « **Libellé** » est le nom par lequel sera appelé le compteur dans le logiciel.

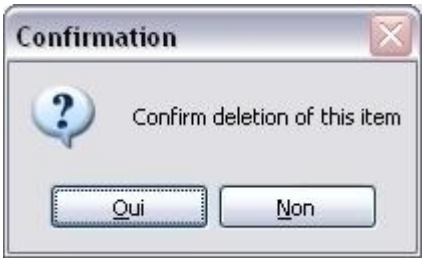
Le champ « **Société** » sert à définir à quelle société appartient l'élément. Certains éléments peuvent appartenir à plusieurs sociétés.

Le champ « **Valeur** » définit la valeur de départ du compteur

<u>Supprimer un Compteur</u>



Sélectionnez le compteur et cliquez sur « Supprimer »



Confirmez la suppression du Compteur

Note : La suppression du Compteur entrainera la suppression de tout le paramétrage associé

Configuration du site

Les périphériques des centrales (suite)

6. Les Automatismes « Centrale »

Les automatismes sont des scénarios utilisés pour déclencher des actions en fonction de conditions préétablies. Ces scénarios sont stockés dans leur centrale au nombre de 32 Automatismes maximum.
Les conditions et actions d'un automatisme sont associées à la même centrale.

Le nom entré dans le champ « **Libellé** », est le nom qui s'affichera pour designer l'automatisme dans tout le logiciel.

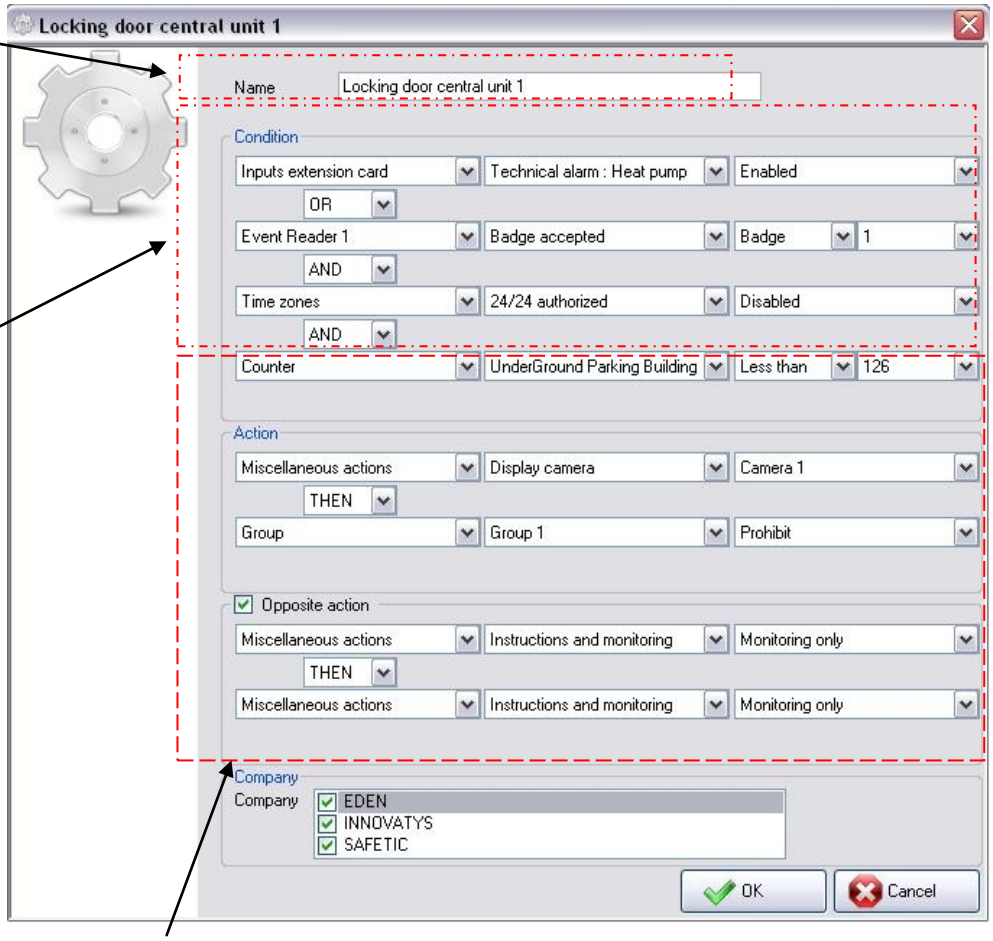
La zone « **conditions** » permet de définir, l'état des paramètres qu'il faudra vérifier pour déclencher l'exécution de l'automatisme. Un automatisme peut contenir jusqu'à 4 conditions.

Les conditions disponibles

1. Plage horaire d'Automatisme,
2. Entrée de la centrale,
3. Entrée d'une carte d'Entrées,
4. Automatisme,
5. Événements de la centrale,
6. Événement d'un Lecteur.
7. État d'un Compteur,
8. État d'un Groupe d'entrées

Il est possible de vérifier que plusieurs paramètres soient vérifiés pour déclencher l'automatisme.
Pour définir comment vérifier les différent paramètres 2 opérateurs logiques sont disponibles : Ou, Et.

Dans le cas du « Ou », il suffit qu'une seule condition parmi toute soit respectée pour déclencher l'automatisme.
Dans le cas du « Et » il faut qu'à un instant « T » toutes les conditions soient respectées.



La zone « **Action** » permet de définir les actions qui seront déclenchées lorsque les conditions seront vérifiées. Un automatisme peut exécuter 2 actions.

Les actions disponibles

1. Sortie,
2. Groupe,
3. Lecteur,
4. Compteur,
5. Actions diverses.
6. Niveau d'alerte,
7. Groupe de sorties,
8. Nombre de passage.

La zone « Action contraire » permet de définir des actions qui se dérouleront lorsque les conditions ne seront plus respectées. Il est possible de créer 2 actions contraires par automatisme.

Configuration du site

Les périphériques des centrales (suite)

6. Les Automatismes « Centrale » (suite)

Conditions d'Automatisme	Description
Plage horaire	Vérification de l'état de la plage horaire activée ou pas
Entrée de la centrale	Vérification de l'état d'une entrée de la centrale NO ou NF
Entrée d'une carte d'Entrées	Vérification de l'état d'une entrée d'une carte d'entrées de la centrale NO ou NF
Automatisme	Vérification du statut de l'automatisme de la centrale
Événements de la centrale	Vérification d'un événement associé à la centrale
Événement d'un Lecteur	Vérification d'un événement associé à un lecteur de la centrale
État d'un Compteur	Vérification du statut d'un compteur de la centrale
État d'un Groupe d'entrées	Vérification de l'état d'un groupe d'entrées de la centrale

Actions d'Automatisme	Description
Sortie	Activation d'une sortie de la centrale ou d'une carte de sortie (impulsion/alternée)
Groupe	Changement de l'état d'un groupe d'accès (Autoriser ou Interdire)
Lecteur	Changement de l'état d'un lecteur la centrale (Mode sous contrôle, Accès Verrouillé, Accès déverrouillé maintenu, ou Accès déverrouillé par Impulsion)
Compteur	Modification de l'état du compteur (Incrémente/décrémente de 1 ou RAZ)
Actions diverses	Remise en cycle des badges, afficher une caméra gérée par un enregistreur vidéo ou afficher une consigne pré-paramétrée
Niveau d'alerte	Modification du niveau d'alerte (Incrémente/décrémente, RAZ ou changement)
Groupe de sorties	Activation d'un groupe de sortie de la centrale (Impulsion ou Alterné)
Nombre de passage	Modification du nombre de passage d'un groupe d'accès sélectionné

Liste des événements pouvant générer des actions

Événement liés à un utilisateur

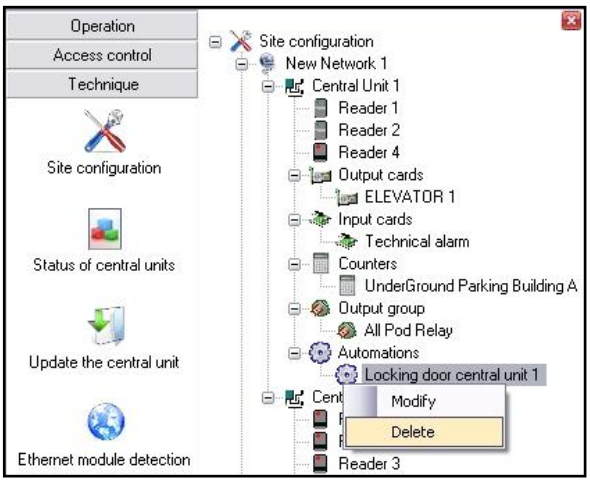
- Utilisateur accepté
- Utilisateur suspendu
- Utilisateur interdit
- Utilisateur inconnu
- Utilisateur déjà rentré
- Utilisateur déjà sorti
- Utilisateur invalide sur la porte
- Utilisateur hors plage horaire
- Utilisateur hors site
- Utilisateur hors distributeur
- Utilisateur sans empreinte
- Erreur format utilisateur
- Groupe interdit
- Badge volé
- Badge sans code
- Badge hors validité
- Badge erroné
- Code accepté
- Code PIN erroné
- Encodage empreinte réussi
- Empreinte alarme utilisée
- Empreinte refusée
- Accompagnateur refusé
- Accompagnateur accepté
- Nombre de passage max atteint
- Utilisateur accepté+attente code
- Utilisateur accepté+attente empreinte
- Utilisateur accepté+attente accompagnateur

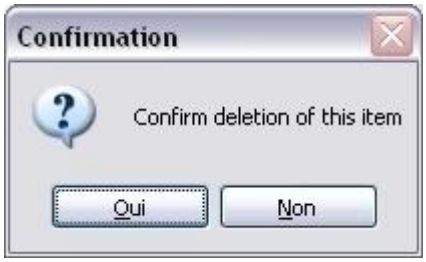
Événement liés à une porte

- Effraction porte
- Fin d'effraction
- Porte verrouillée
- Porte bloquée
- Fin porte ouverte
- Ouverture sur BP
- Délai de saisie code dépassé
- Erreur écriture badge
- Véhicule non détecté
- Plaque non reconnue
- Délai transit dépassé
- Ouverture impulsionnelle par GTC
- Ouverture maintenue par GTC
- Fermeture maintenue par GTC
- Commande mode Auto GTC
- Ouverture porte sur début plage accès libre
- Fermeture porte sur fin plage accès libre
- Plaque reconnue en attente de badge
- Délai accompagnateur dépassé

Événement liés au système

- Hors condition
- Capteur sale
- Clavier bloqué
- Fin de blocage clavier
- Effraction boîtier
- Fin d'effraction boîtier
- Défaut power
- Fin défaut power
- Effraction boîtier BIO
- Fin d'effraction boîtier BIO
- Exécution automatisme
- Fin d'exécution automatisme
- Changement de niveau d'alerte
- Connexion bus d'extension
- Déconnexion bus d'extension
- Arrachement Boîtier BIOVEIN
- Fin d'arrachement BIOVEIN
- Mise en service alarme (mode bistable)
- Mise hors service alarme (mode bistable)
- Impulsion ON/OFF alarme





Confirmez la suppression du compteur
La suppression du compteur entrainera la suppression de tout le paramétrage associé

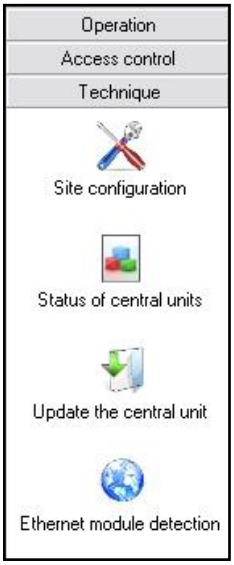
Les « automatismes Centrale » ne peuvent générer d'action entre les centrales. Pour cela il faut utiliser les « Automatismes centralisés » managés par le logiciel (voir page 65)

Configuration du site

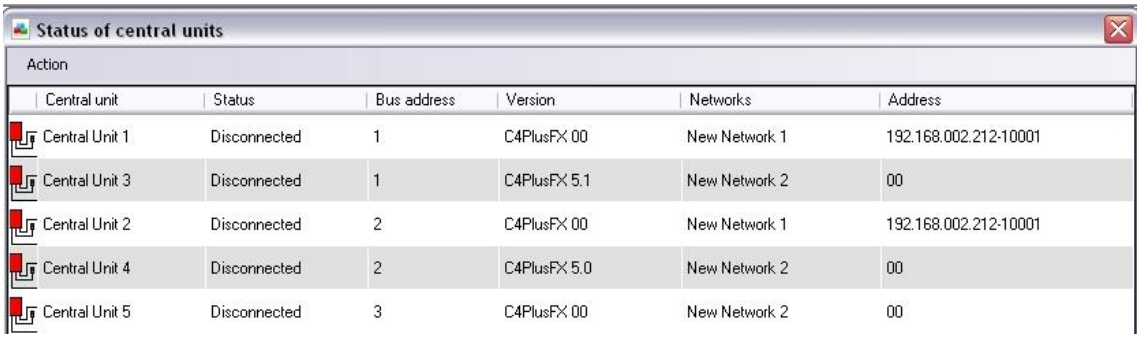
Etat des centrales

Sélectionnez le menu Technique → État des centrales

La fenêtre d'état des centrales permet d'avoir un aperçu du statut de chaque centrale de l'installation



Sélectionnez l'onglet « Technique » et cliquer sur« État des centrales »


Status of central units
Action
Central unit | Status | Bus address | Version | Networks | Address
Central Unit 1 | Disconnected | 1 | C4PlusFX 00 | New Network 1 | 192.168.002.212-10001
Central Unit 3 | Disconnected | 1 | C4PlusFX 5.1 | New Network 2 | 00
Central Unit 2 | Disconnected | 2 | C4PlusFX 00 | New Network 1 | 192.168.002.212-10001
Central Unit 4 | Disconnected | 2 | C4PlusFX 5.0 | New Network 2 | 00
Central Unit 5 | Disconnected | 3 | C4PlusFX 00 | New Network 2 | 00

La première colonne affiche une icône dont la couleur dépend du statut de la centrale.
La deuxième colonne affiche le libellé de la centrale.
La colonne statut indique l'état dans lequel se trouve la centrale.

La colonne « Version » affiche le type de centrale déclaré, et la version de la centrale détectée par le logiciel. Tant que la communication entre le logiciel et la centrale n'est pas établie, la version de la centrale restera en « v 0.0 ».
La colonne « Réseau » indique le libellé du réseau sur lequel la centrale est connectée.
La colonne « Adresse » affiche le type de réseau sur lequel est branchée la centrale ainsi que son adresse.

Nominale : c'est l'état dans lequel se trouve les centrales lorsque la communication entre l'ordinateur et celles-ci est établie. Nominale est l'état courant dans lequel doivent se trouver les centrales.

Initialisation en cours : Une centrale affiche cet état, lors de sa première connexion avec un ordinateur, lors d'une reprogrammation ou lorsqu'une demande d'initialisation manuelle est demandée par l'utilisateur. L'icône est rouge

Paramétrage en cours : Ce statut est affiché lorsque l'ordinateur envoi des données à une centrale.
Dans ce statut, aucun événement ne remonte sur l'ordinateur. L'icône est verte.

Occupée : cet état est affiché lorsque des données transitent de la centrale vers l'ordinateur.

Réseau indisponible : La centrale est dans cet état lorsque l'ordinateur ne parvient pas à entrer en communication avec l'interface (type C485FX, MODTCP/IP…). L'icône de la centrale est Rouge.

Déconnectée : L'état déconnecté est affiché lorsque la communication entre l'ordinateur et l'interface est établie, mais que l'interface ne parvient pas à entrer en communication avec les centrales.

Version Incompatible : L'ordinateur affiche ce statut lorsque la version du logiciel et celle du firmware de la centrale sont incompatible. Dans ce cas une mise à jour de la centrale est nécessaire.

Type incompatible : Cet état indique une mauvaise déclaration du type de la centrale qui est présente à cette adresse. L'icône de la centrale apparait en jaune.
La colonne « Adresse Bus » indique l'adresse que la centrale occupe sur le bus. Un bus peut comporter jusqu'à 32 centrales.

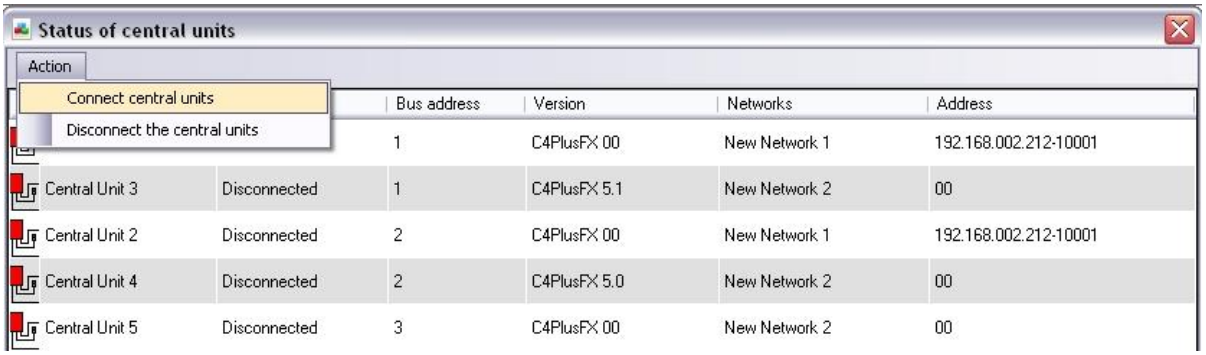
Ecriture Flash : Mise à jour du firmware en cours.

Configuration du site

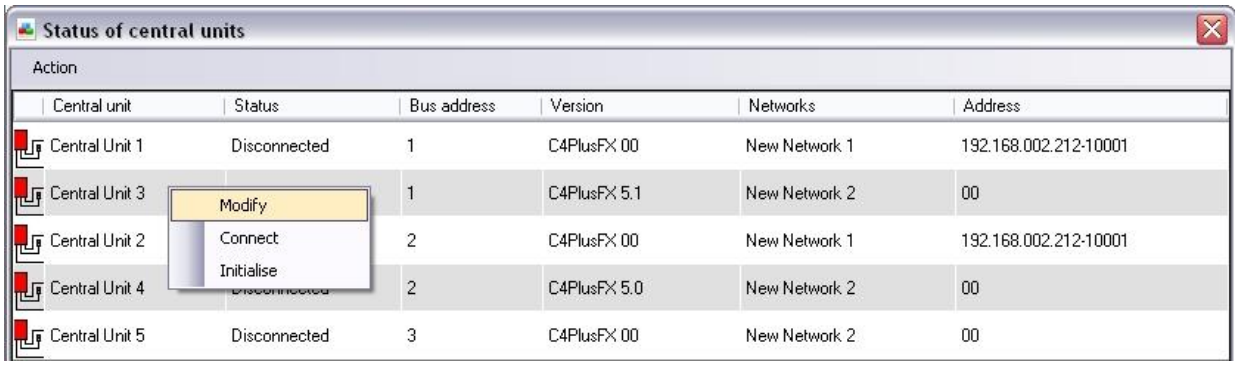
Etat des centrales (suite)

Il est possible d'interrompre ou d'activer la communication avec toutes les centrales à la fois en se servant du menu "Action".

L'action "Déconnecter" aura pour effet de passer les centrales en mode "Hors connexion" et désactiver la communication alors que "Connecter" activera la communication avec les centrales.



Vous pouvez également initialiser, afficher la page des paramètres d'une centrale ou la déconnecter/connecter en faisant directement un clic droit sur la ligne affichant les informations de cette centrale :



Configuration du site

Mettre à jour la centrale

La mise à jour du firmware de la centrale, permet l'installation d'un nouveau firmware sur les centrales de l'installation.

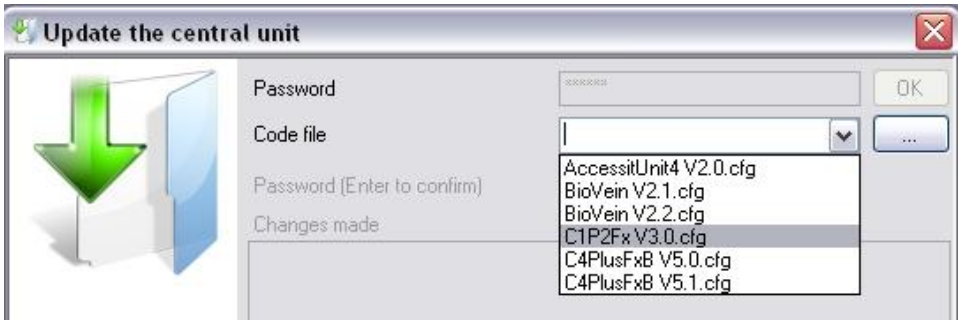
La mise à jour du firmware peut être nécessaire lorsque le logiciel indique « version incompatible » dans le menu « l'état des centrales ».
Les versions de centrales compatibles avec le logiciel sont:

- C1P2FX v3.0 et supérieurs
- C4PlusFX v5.0 et supérieurs
- Genius v2.0 et supérieurs
- BioVein v2.0 et supérieurs

Le logiciel ne propose pas des mises à jour automatiques des centrales, mais toutes les centrales inférieures à ces versions seront en état « version Incompatible » et l'utilisateur doit utiliser le procédure de mise à jour des centrales

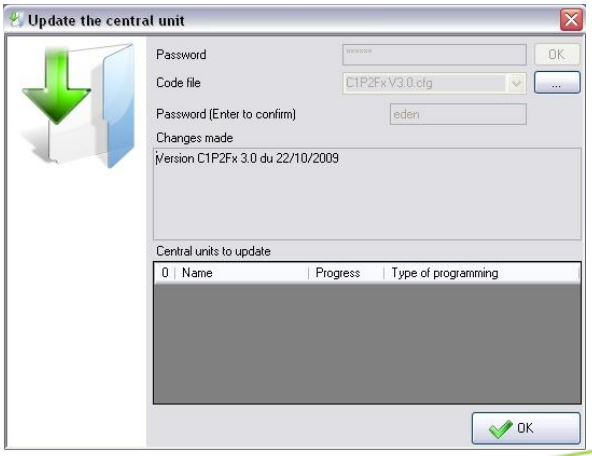
Procédure

1.Éditez le mot de passe « edenfx ».
2. Validez par le bouton « OK ».
3. Sélectionnez dans le menu déroulant le firmware de la centrale à mettre à jour.
4.Éditez le mot de passe « eden ».
5. Validez par la touche « entrée » du clavier/PC.
6. Sélectionnez la centrale à mettre à jour.
7. Pour lancer le MAJ, cliquez sur OK.



8. Laissez le logiciel effectuer la mise à jour des centrales sélectionnées.

9. Réitérez la même procédure pour les autres modèles de centrales de l'installation si nécessaire.

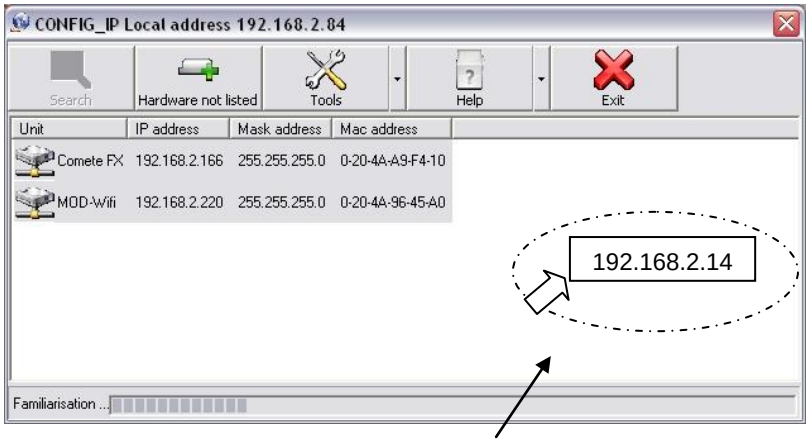


Pour tout complément d'information sur la nécessité d'une mise à jour de centrale de votre installation, contactez notre hotline **:** **hotline@eden-innovations.com**

Configuration du site

Détection modules Ethernet

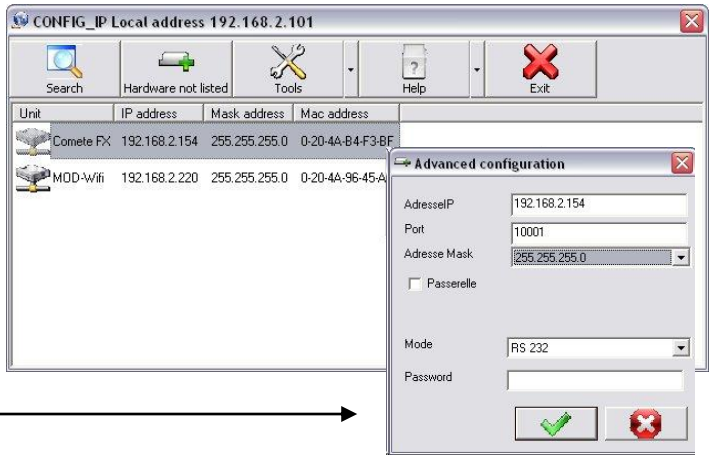
Sélectionnez l'onglet « Technique » → Détection modules Ethernet



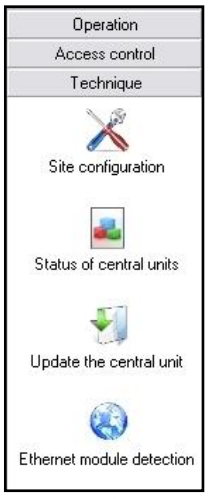
Il est possible d'effectuer l'action « glisser/déplacer » de l'adresse IP, à partir de la fenêtre « Config IP » vers le champ « Adresse IP » de la fenêtre « Réseau ».
Pour modifier le paramétrage d'un des matériels, faites un clic droit sur la ligne concernée. Un menu contextuel apparait.

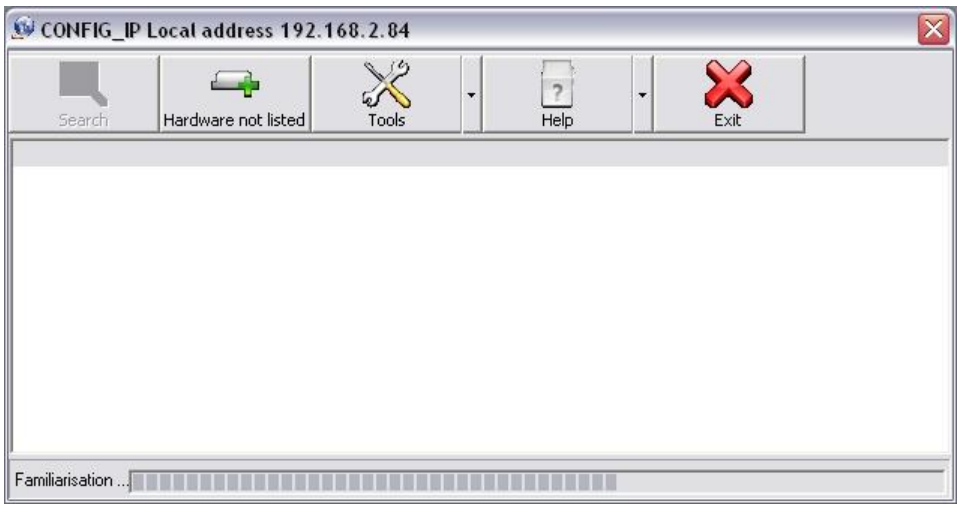
Choisissez « configurer » pour faire apparaitre une nouvelle fenêtre.

Le champ se remplit alors automatiquement



Laissez le mode en RS 232 ⟶





La détection des modules Ethernet « EDEN » se lance systématiquement
Le bouton « Rechercher » lance la détection automatique du matériel présent sur le réseau Ethernet.

Configuration du site

Les automatismes « centralisés »

Sélectionnez l'onglet « Contrôle d'accès » → automatismes « centralisés »

Les automatismes sont des scénarios utilisés pour déclencher des actions en fonction de conditions préétablies. Les automatismes centralisés sont stockés dans le serveur du logiciel et peuvent générer des actions entre les centrales du site.

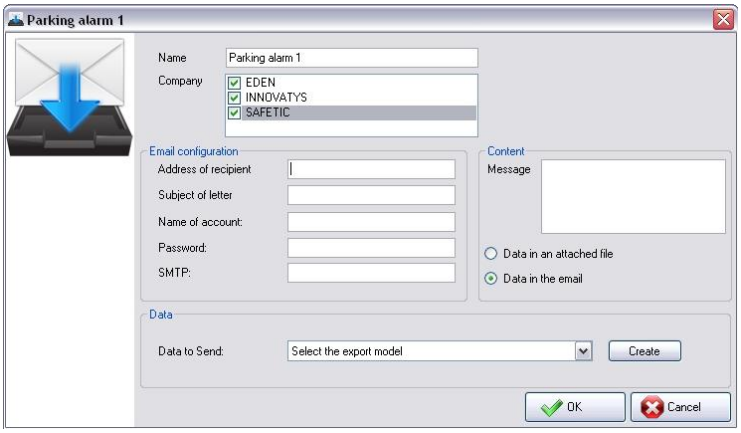
Ces automatismes nécessitent que le PC Serveur reste allumé. L'interface client peut être fermée, ainsi que la session Windows.

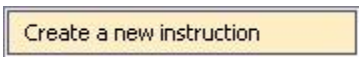
1. Les compteurs globaux, Emails, Exportations et consignes

- Sélectionnez l'onglet « Contrôle d'accès »
- Cliquez sur « automatismes centralisés »
- Sélectionnez « Compteurs globaux »
- Cliquez sur « Créer un compteur Global »

- Editez le nom du compteur global qui s'affiche dans le logiciel. Le champ « valeur » permet d'éditer une valeur d'origine au compteur.
- Sélectionnez la ou les sociétés qui pourront gérer ce compteur.

-Éditez le nom de l'Email qui s'affichera dans le logiciel.
- Sélectionnez la ou les sociétés qui pourront gérer cet email.
- Éditez l'adresse mail du destinataire
- Éditez l'objet du courriel
- Éditez le nom du compte mail du destinataire
- Éditez son mot de passe
- Éditez le nom de son serveur SMTP, suivi du port (ex : smtp.gmail.com :587)
- Sélectionnez dans le menu déroulant les données à envoyer dans le corps du mail ou en pièce-jointe.





- Editez le nom de la consigne qui s'affichera dans le logiciel.
- Editez la consigne.
- Sélectionnez la ou les sociétés qui pourront gérer cette consigne.

Configuration du site

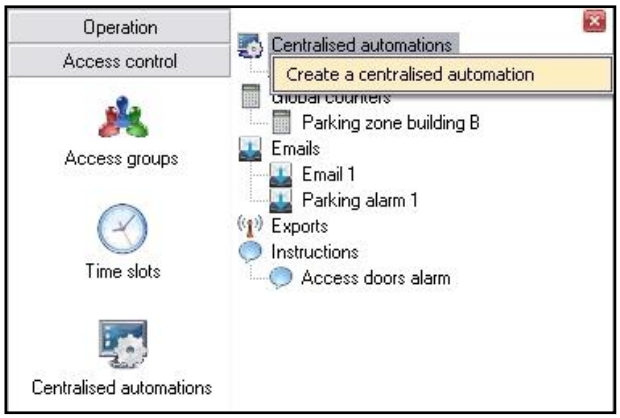
Les automatismes « centralisés » (suite)

Sélectionnez l'onglet « Contrôle d'accès » → automatismes « centralisés »

2. Édition des automatismes « Centralisés »

Rappel de la constitution d'un Automatisme « Centralisé »

- Conditions avec paramètres « ou » « et » + actions et actions contraires
- Nombre d'automatismes illimités



- Sélectionnez l'onglet « Contrôle d'accès »
- Cliquez sur automatismes « centralisés »
- Créez un automatisme centralisé

Processus

1.Éditez un nom pour l'automatisme

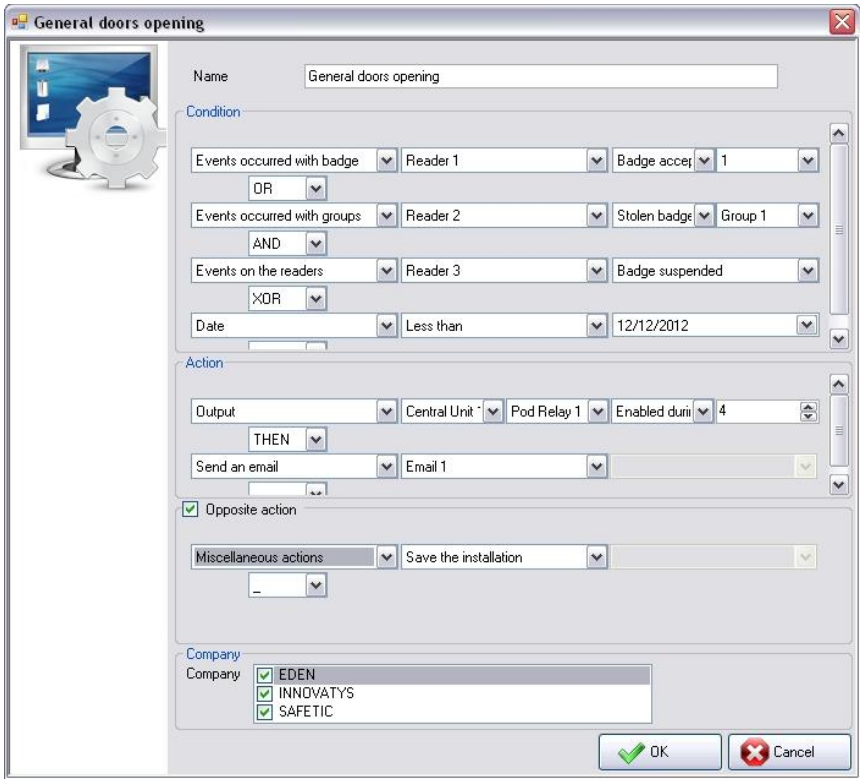
2. A l'aide des menus déroulants, sélectionnez les conditions qui serviront pour déclencher les actions souhaitées. Les conditions, une fois vérifiées, déclencheront l'automatisme.

Les conditions peuvent être cumulées par l'intermédiaire d'opérateurs logiques « ET, OU et XOR ».

3. Sélectionnez les actions souhaitées à l'aide des menus déroulants.

Les actions permettent de définir ce qui se passera lorsque les conditions seront vérifiées.

4. Sélectionnez les actions contraires. Les actions contraires permettent de définir une action à exécuter lorsque les conditions ne seront plus respecter.



L'exécution d'un automatisme centralisé peut être directement forcée depuis le menu « supervision ».

Configuration du site

Les automatismes « centralisés » (suite)

Sélectionnez l'onglet « Contrôle d'accès » → automatismes « centralisés »

Conditions d'Automatisme	Description
Aucune Condition	Vérifie qu'il n'y ait pas de condition pour déclencher les actions
Badge	Vérifie le statut d'un badge (En service, Suspendu ou Volé)
Événement lié a un badge	Vérifie l'événement suite au passage d'un badge sur un lecteur
Groupe	Vérifie le statut d'un groupe d'accès (Autorisé ou Interdit)
Événement lié à un groupe	Vérifie un événement suite au passage d'un badge d'un groupe d'accès identifié sur un lecteur
Lecteur	Vérifie l'état d'un lecteur (mode Auto, Ouverture/Fermeture Maintenue)
Événement lié à un lecteur	Vérifie le statut d'un compteur de la centrale
Date	Vérifie la valeur d'une date
Heure	Vérifie la valeur d'une heure
Plage horaire	Vérifie l'état d'une plage horaire
Zone	Vérifie l'état d'un compteur de présence des utilisateurs d'un groupe d'accès dans une zone
Groupe présent en mn dans une zone	Vérifie l'état d'un compteur de temps d'un groupe d'accès dans une zone
Automatisme « Centrale »	Vérifie l'état d'un automatisme « local »
Compteur	Vérifie l'état d'un compteur local (stocké dans une centrale)
Compteurs « Globaux »	Vérifie de l'état d'un compteur global (stocké dans le serveur du logiciel)
Entrée d'alarme GALAXY	Vérifie de l'état d'une entrée d'alarme d'une centrale GALAXY
Groupe d'entrées GALAXY	Vérifie de l'état d'un groupe d'entrées d'alarme d'une centrale GALAXY
Sortie relais GALAXY	Vérifie de l'état d'une sortie relais d'une centrale GALAXY

Configuration du site

Les automatismes « centralisés » (suite)

Sélectionnez l'onglet « Contrôle d'accès » → automatismes « centralisés »

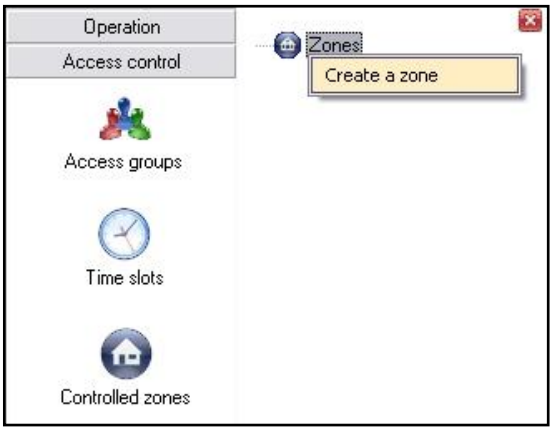
Actions d'Automatisme	Description
Sortie	Active une sortie d'une centrale ou d'une carte de sortie (impulsion/alternée)
Lecteur	Change l'état d'un lecteur (Mode sous contrôle, Accès Verrouillé, Accès déverrouillé maintenu, ou Accès déverrouillé par Impulsion)
Groupe	Change l'état d'un groupe d'accès (Autoriser ou Interdire)
Badge	Change l'état d'un badge (En service, Suspendu, profil 0, 1 ou 2)
Vider Zone	Vide la liste utilisateurs présents dans une zone sélectionnée
Camera vidéo analogique	Affiche une caméra ou la préposition d'un dôme relié à un DVR
Camera IP	Affiche une caméra ou la préposition d'un dôme IP
Compteur	Modifie de l'état d'un compteur local (Incrémente/décrémente de 1 ou RAZ)
Compteur global	Modifie de l'état d'un compteur global (Incrémente/décrémente de 1 ou RAZ)
Consigne	Affiche une consigne de sécurité
Exécuter automatisme centralisé	Exécute d'un automatisme centralisé
Historique	Exécute une requête d'historique
Envoyer un mail	Envoie un courriel
Exporter vers un fichier	Exporte un fichier de données
Entrée GALAXY	Change l'état d'une entrée d'alarme Intrusion d'une centrale GALAXY
Groupe GALAXY	Change l'état d'un groupe d'entrées d'alarme Intrusion d'une centrale GALAXY
Sortie relais GALAXY	Change l'état d'une sortie relais d'une centrale GALAXY
Actions diverses	Sauvegarde la base de données du serveur

Configuration du site

Les Zones contrôlées

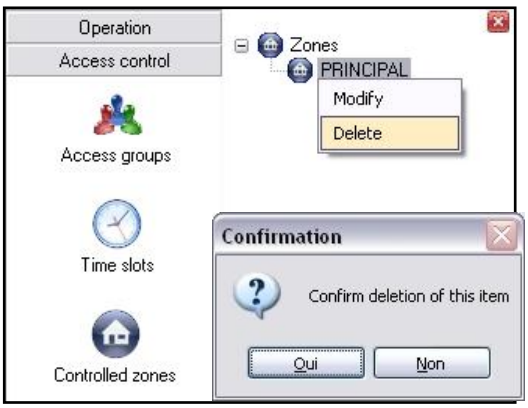
Sélectionnez « Contrôle d'accès »→ Zones contrôlées

- Une zone est un espace délimité par un ou plusieurs lecteurs d'entrée et un ou plusieurs lecteurs de sortie.
- A une zone peut être associé un comptage ou une gestion du temps de présence qui permet de se renseigner sur l'occupation instantanée de cette zone.



Procédure

1. Éditez le nom de la zone
2. Sélectionnez le ou les lecteurs d'entrée de cette zone
3. Sélectionnez le ou les lecteurs de sortie de cette zone
4. Sélectionnez la ou les sociétés/locataires qui pourront gérer cette zone



La suppression de cet élément entrainera la suppression de tout le paramétrage associé

Une zone peut avoir un nombre inégal de lecteur de type « Entrée »et de type « Sortie ».

La création de cette zone permettra de connaître les utilisateurs présents en temps réel via le menu « Occupation des zones » (page 108).

Il est possible aussi d'utiliser cette zone pour connaitre le cumul de temps de présence d'un groupe d'utilisateur suivant des requêtes calendaires via le menu « temps de présence » (page 107).

Chapitre 4

Les droits d'accès

Que contient ce chapitre ?

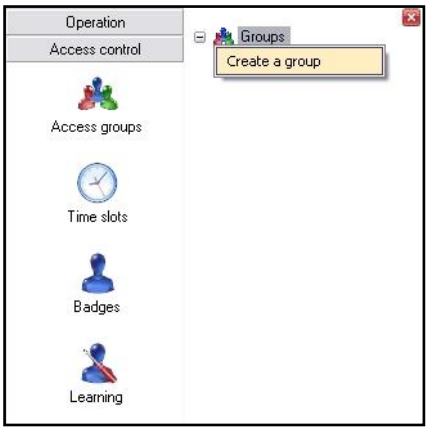
Les droits d'accès ..... Erreur ! Signet non défini.
Les Groupes d'accès 70
Les plages horaires 71
1. Les plages horaires « Utilisateur » 71
2. Les plages horaires « Automatismes » 72
3. Les jours fériés 73

Les droits d'accès

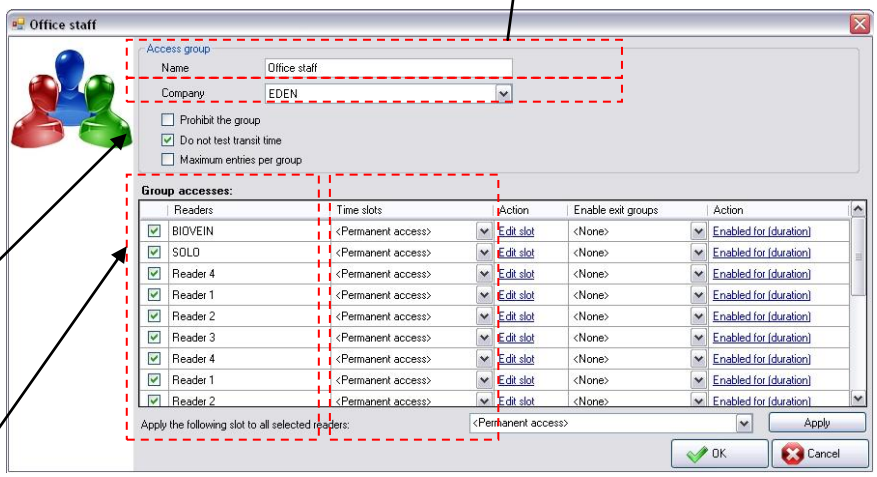
Les Groupes d'accès

Sélectionnez Contrôle d'accès → Groupes d'accès

- Les groupes d'accès permettent de définir les autorisations d'accès des utilisateurs sur le site.
- Un groupe est composé d'un ou plusieurs lecteurs et peut être modifié à tout instant.
- Vous pouvez créez jusqu'à 1024 groupe d'accès dans le logiciel.



« champs libellé »
Éditez le nom du groupe d'accès qui s'affichera dans tout le logiciel.



Champ **« société »** permet de définir à quelle société appartient le groupe.
Vous ne pouvez associer un groupe qu'à une seule société.

Champ **« lecteur »**
Cochez les cases des lecteurs souhaités.

Champ **« Plage horaire »**
Une fois les lecteurs validés, vous pouvez sélectionnez une plage horaire pour chaque.

« **Accès permanent** » permet de donner accès sur un lecteur sans restriction.

« **Éditer la plage** » permet de modifier la plage sélectionnée ou d'en créer une autre si "<Accès permanent>" est sélectionné.

Champ **« appliquer la plage suivante à tous les lecteurs cochés** » permet d'affecter une même plage horaire à tous les lecteurs autorisés pour le groupe.

La case **« Interdire le groupe »**, empêche lorsqu'elle est cochée, l'utilisation de tous les badges faisant partis du groupe.

La case **« Ne pas tester le délai de transit »** permet en cas d'utilisation de la fonction délai de transit sur l'installation, d'autoriser le groupe à ne pas être soumis à ce contrôle.

L'option **« Utiliser le maximum par groupe »** permet de définir un nombre maximum de personnes du groupe qui passe sur un lecteur défini en entrée.

« Activer Groupes de sorties » permet d'activer pendant un temps donné des groupes de sorties lors du passage d'un badge associé à ce groupe sur le lecteur correspondant.
Cette fonction est utilisée pour la gestion d'étage dans un ascenseur, par exemple.

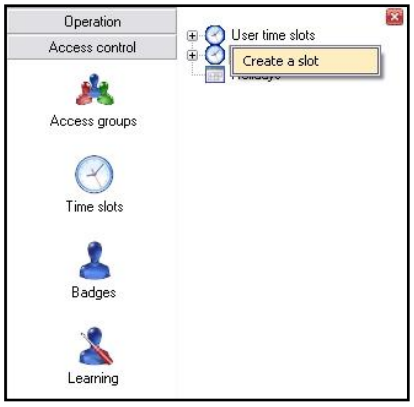
Les droits d'accès

Les plages horaires

Sélectionnez Contrôle d'accès → Plages horaires → Plages horaires « Utilisateur »

1. Les plages horaires « Utilisateur »

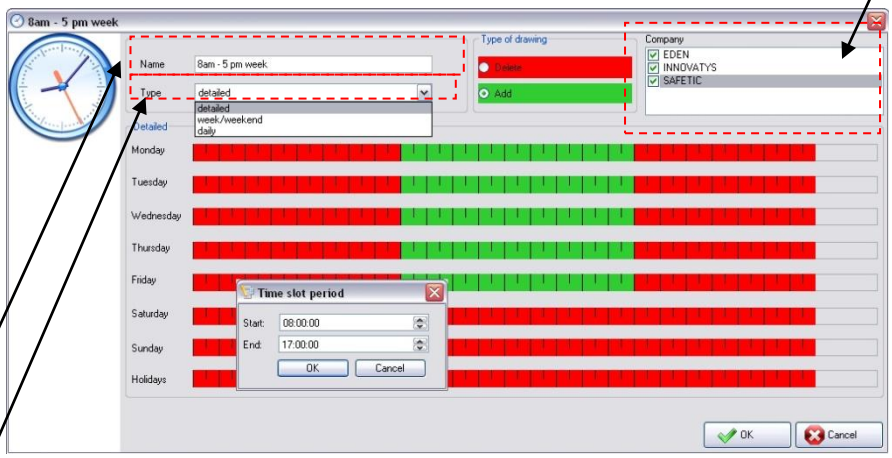
- Une plage horaire permet de définir des créneaux « Autorisés » et « Interdits » qui seront associées aux « badges/ utilisateurs » et aux « Groupe d'accès ».
- Vous pouvez créer jusqu'à 64 plages horaires et 10 créneaux par jour.
- Chaque créneau horaire est paramétrable à la minute.
- Un créneau ne peut pas être inférieur à 5 minutes.



Champ **« Libellé »**
Éditez le nom de la plage horaire qui
s'affichera dans le logiciel.

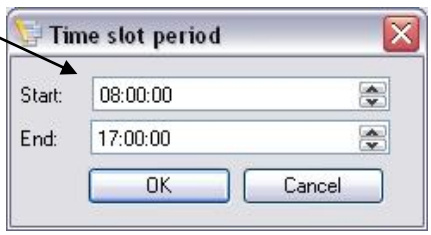
Champ **« Type »**
Sélectionnez le profil d'édition de la plage horaire.

Champ**« Société » :**
Permet de définir à quelle société appartient la plage horaire.



Le type de dessin permet de définir si le créneau sera autorisé (en vert) ou interdit (en rouge).
Pour créer un nouveau créneau horaire, cliquez sur la ou les barres sur lesquelles le créneau doit être créé et de déplacez la souris tout en maintenant le bouton gauche.
Les heures de début et de fin de créneau, s'affichent au bout de chaque barre.

Pour définir précisément les horaires, il est possible de faire un clic droit sur un des créneaux et de choisir modifier. Une fenêtre apparait alors, et vous permet de définir l'heure de début et l'heure de fin de créneau.



Une plage supplémentaire est disponible, c'est la plage jour férié. La plage jours fériés s'applique durant les jours qui ont été définis comme fériés.

<u>3 profils distincts</u>
« **Quotidienne** »,
La même plage horaire est appliquée
pour tous les jours de la semaine.

« **Semaine/Week-end** »,
Une plage horaire pour la semaine et
une autre pour le week-end.

« **Détaillée** »
7 plages horaires par semaine.

Les droits d'accès

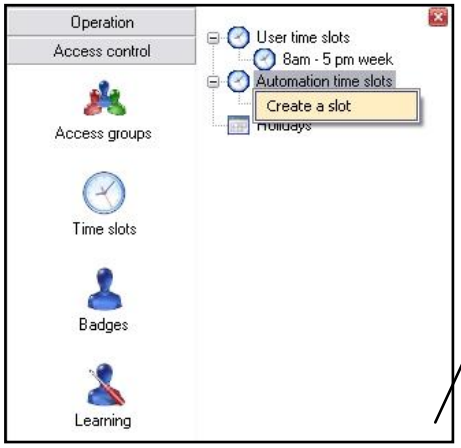
Les plages horaires

Sélectionnez Contrôle d'accès → Plages horaires → Plages horaires « Automatismes »

2. Les plages horaires « Automatismes »

- Une plage horaire permet de définir des créneaux « Autorisés » et « Interdits » qui seront associées aux scénarios appelé « Automatisme » et aux lecteurs pour la fonction « Accès libre ».
- Vous pouvez créer jusqu'à 64 plages horaires et 10 créneaux par jour.
- Chaque créneau horaire est paramétrable à la minute.

Un créneau ne peut pas être inférieur à 5 minutes.

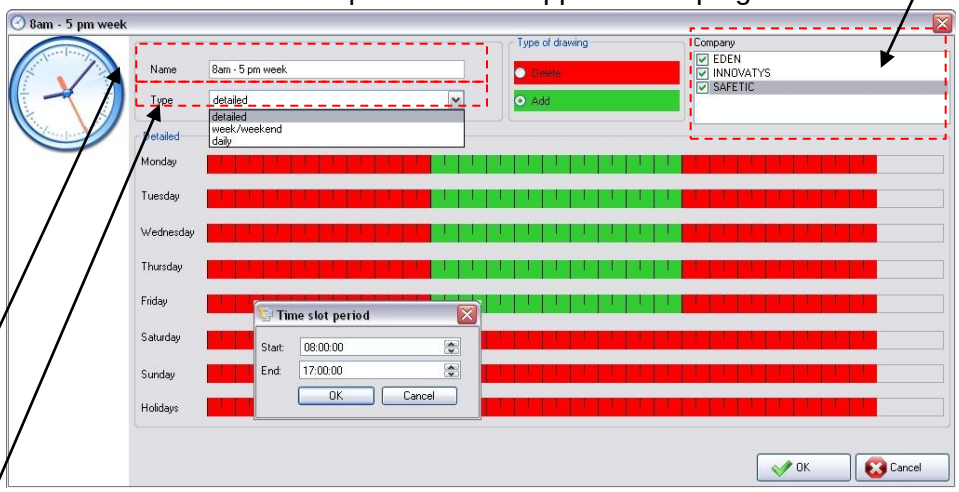


Champ **« Libellé »**
Éditez le nom de la plage horaire qui
s'affichera dans le logiciel.

Champ **« Type »**
Sélectionnez le profil d'édition de la plage horaire.

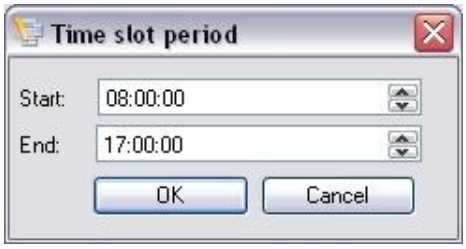
<u>3 profils distincts</u>
« **Quotidienne** »,
La même plage horaire est appliquée
pour tous les jours de la semaine.
« **Semaine/Week-end** »,
Une plage horaire pour la semaine et
une autre pour le week-end.
« **Détaillée** »,
7 plages horaires par semaine.

Champ**« Société » :**
Permet de définir à quelle société appartient la plage horaire.



Le type de dessin permet de définir si le créneau sera autorisé (en vert) ou interdit (en rouge).
Pour créer un nouveau créneau horaire, cliquez sur la ou les barres sur lesquelles le créneau doit être créé et de déplacez la souris tout en maintenant le bouton gauche.
Les heures de début et de fin de créneau, s'affichent au bout de chaque barre.

Pour définir précisément les horaires, il est possible de faire un clic droit sur un des créneaux et de choisir modifier. Une fenêtre apparait alors, et vous permet de définir l'heure de début et l'heure de fin de créneau.



Une plage supplémentaire est disponible, c'est la plage jour férié. La plage jours fériés s'applique durant les jours qui ont été définis comme fériés.

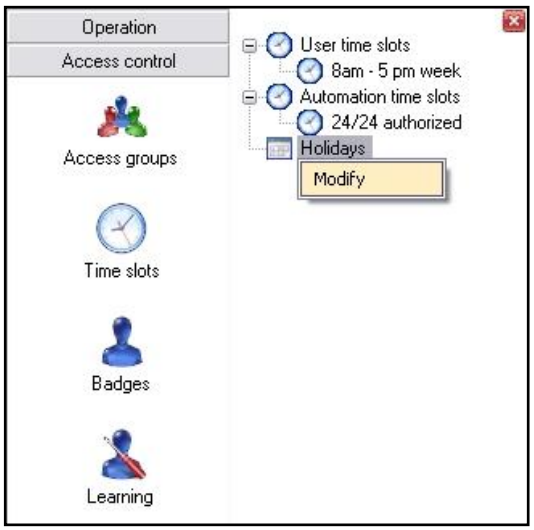
Les droits d'accès

Les plages horaires

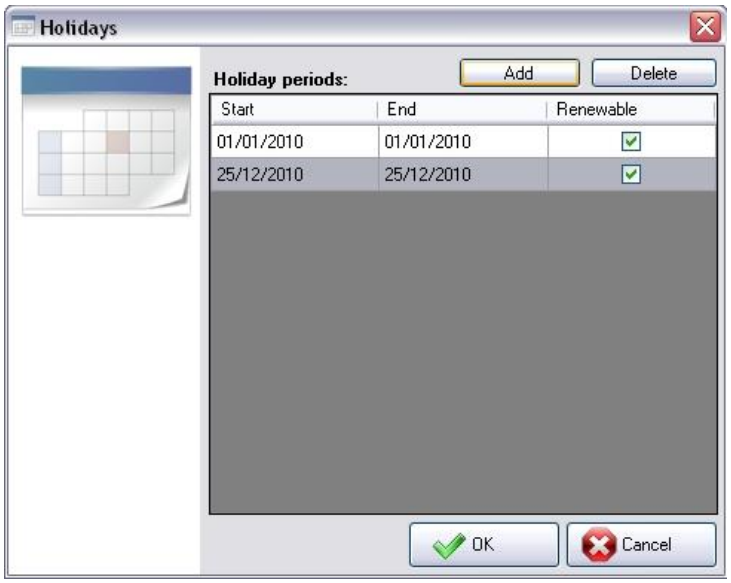
3. Les jours fériés

Sélectionnez Contrôle d'accès → Plages horaires → Jours fériés

- Le planning annuel permet de définir des « périodes de jours fériés » devant être gérées par le contrôle d'accès.
- Ces jours-là sont prioritaires quel que soit le jour de la semaine, les horaires définis en jours fériés sont appliqués pour les badges ne disposant pas d'un accès permanent.
- L'on peut créer 32 périodes de jours fériés sans limite du nombre de jour par période.



Cliquez sur « Jours fériés puis modifier »



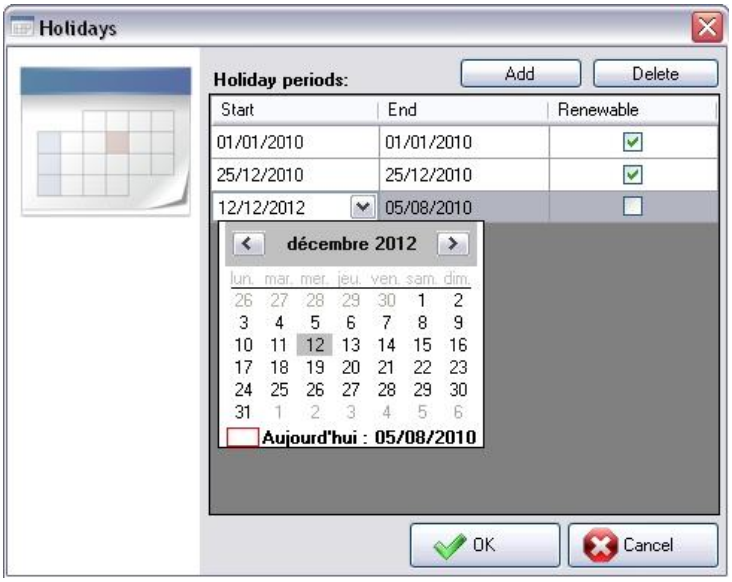
Une période de jours fériés est définie en cliquant sur le bouton « **Ajouter** »

Choisissez le jour de début et de fin sur la nouvelle ligne.
Il n'y a pas de limite du nombre de jour pour la même période

Un jour férié est renouvelable tous les ans si l'on coche la case de la ligne correspondante.

Pour effacer un jour férié, il faut se placer sur la ligne correspondante et cliquer sur "Supprimer".

Les jours fériés sont automatiquement mis à jour dans les centrales tous les jours à condition que ces dernières soient connectées à l'ordinateur.



Chapitre 5

Les utilisateurs et les badges

Que contient ce chapitre ?

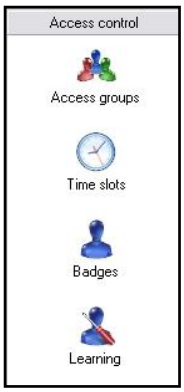
Les utilisateurs et les badges 74
Créer une nouvelle série de badges 75
Liste des badges/utilisateurs 76
Apprentissage des badges 77
Personnalisation du Badge 78
Modèle de badge imprimable 79
La fiche badge/utilisateur 80
1.Le profil « standard » 80
2.Les profils « additionnels » 81
3.L'onglet « Options » 82
4.L'onglet « Informations complémentaires » 83
5.L'onglet « Enrôlement » 84
6.L'onglet « Encodage » 85
7.L'onglet « Impression » 86
8.Récupération rapide des données 87

Les utilisateurs et les badges

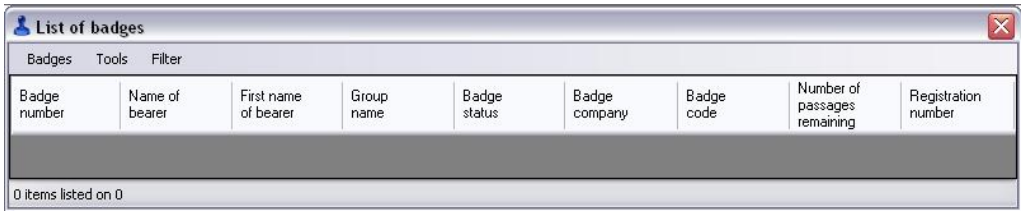
Créer une nouvelle série de badges

Sélectionnez Contrôle d'accès → Badges → Liste des badges

- Ce menu permet la création, modification et suppression de badges et utilisateurs du site.
- La liste des badges affiche la liste complète ou filtrée des badges et utilisateurs qui ont été paramétrés sur le site.
- Un clic droit sur un badge permet de modifier (ouvre la fiche badge) ou de supprimer le badge en question.
- Un double-clic sur un badge a le même effet que l'option "modifier".



- Sélectionnez l'onglet « Contrôle d'accès »
- Cliquez sur « Badges »



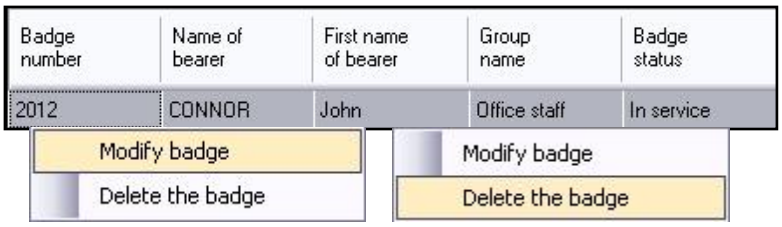
Cliquez sur « Ajouter une série de badges »

<u>Description des champs</u>

Premier badge : numéro du premier badge de la série
Quantité : quantité de badges à créer
Statut : statut des badges à créer
« En service », « Suspendu » ou « Volé »
Groupe : groupe d'accès auquel les badges créés seront affectés
Afficher le groupe: affichera le groupe d'accès sélectionné
Utilisateurs à enrôler : indique si les badges créés devront permettre l'enrôlement biométrique de l'utilisateur au premier passage sur un lecteur.
Type de série : définit si les badges créés auront un nombre de passages maximum ou pas
Nombre de passages : indique le nombre de passages autorisés
de la série de badge
Société : si plusieurs sociétés ou locataires sont définies, indiquez la société des badges à créer.

Pour « **modifier** » la fiche badge/utilisateur il faut sélectionner la ligne correspondante et effectuer un clic droit, puis « modifier le badge »

Pour « **supprimer** » la fiche badge/utilisateur il faut sélectionner la ligne correspondante et effectuer un clic droit, puis « supprimer le badge » Une confirmation vous sera demandée.



Les utilisateurs et les badges

Liste des badges/utilisateurs

Sélectionnez Contrôle d'accès → Badges → Liste des badges

Ce menu permet d'effectuer différents traitements sur une liste des badges et utilisateurs enregistrés dans le système.

Menu "**Outils**"

« Traitements groupés »
Affecter ou modifie des propriétés à plusieurs badges en même temps

« Copier vers le presse-papier »
Copie la liste de badge affichée dans le presse-papier de Windows

« Supprimer une série de badge »
Supprime une série de badges définie

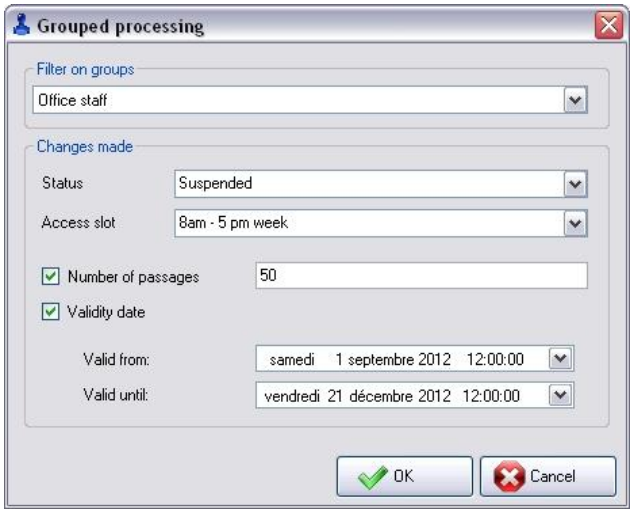
« Filtre des groupes »
Sélectionne un
groupe d'accès afin de modifier des paramètres.

« Statut »
Modifie le statut de tous les badges/utilisateurs associés au groupe sélectionné.
Statuts disponibles = En service, Suspendu et Volé

« Plage d'accès »
Affiche la liste de toutes les plages utilisateurs disponibles

« Nombre de passages »
Modifie/ajoute un crédit de passage à tous les utilisateurs associés à ce groupe

« Date de validité »
Modifie/affecte une date de début/fin de validité pour tous les utilisateurs associé au groupe sélectionné



« Supprimer une série de badge »
Ce menu permet de supprimer une série de badges comprises entre deux numéros paramétrables.

Le menu « Filtre » permet de filtrer la liste des badges suivant le formulaire de recherche de badge; pour afficher à nouveau tous les badges, cliquez sur "Effacer les filtres".

« Recherche d'un badge »
Ce menu permet de filtrer l'affichage de la liste des badges suivant différents critères et champs de la base de données de la fiche badge/utilisateur.

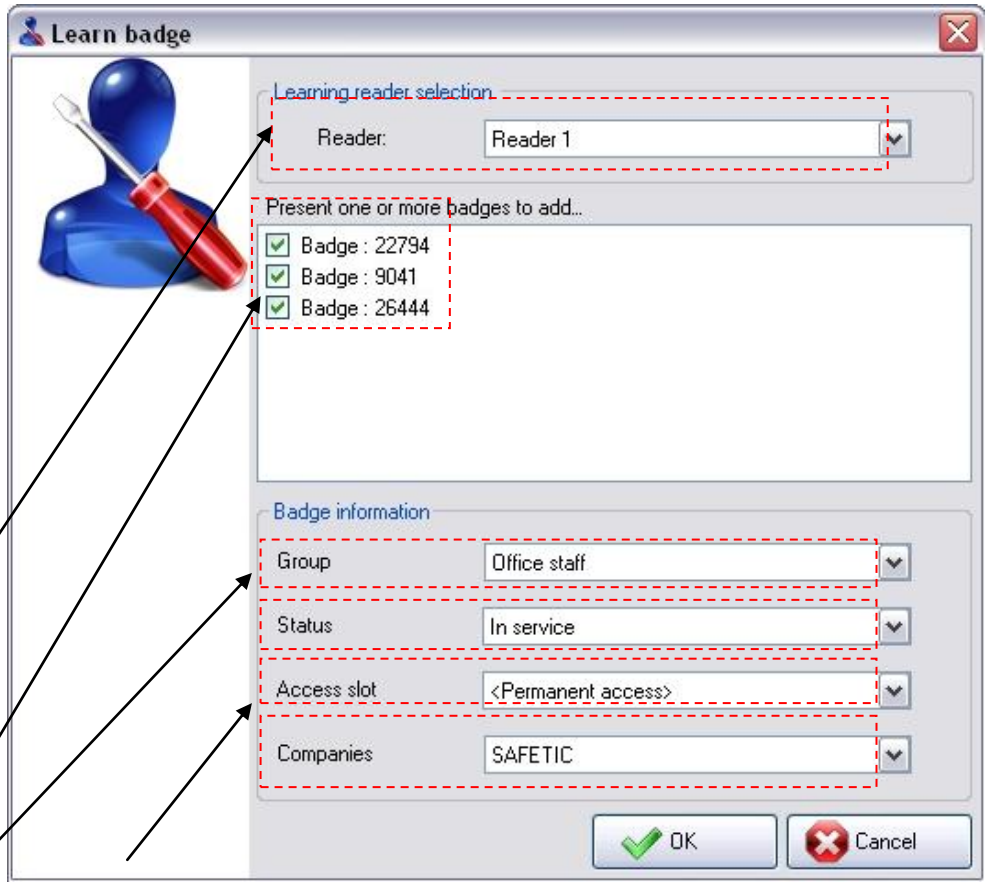
Les critères sont: N° de badge, Nom du porteur + tous les champs personnalisés de la fiche du badge/utilisateur.

Les utilisateurs et les badges

Apprentissage des badges

Sélectionnez Contrôle d'accès → Apprentissage

Cette fonction permet d'enrôler les badges en les passant devant un des lecteurs du site afin de les enregistrer dans la base de données du logiciel. Cela peut aussi éviter les erreurs de lecture des numéros des badges imprimés.



Choix du lecteur d'apprentissage

« Lecteur »
Ce menu déroulant permet de sélectionner le lecteur qui va servir à enrôler les nouveaux badges parmi tous les lecteurs du site.
Après leur passage sur le lecteur sélectionné, les nouveaux badges s'afficheront dans la fenêtre.

Informations badges

« Groupe »
Ce menu déroulant permet de sélectionner et d'affecter un des groupes d'accès existant au badge et à l'utilisateur nouvellement enrôlé.

« Statut »
Affecter un statut pour le badge et l'utilisateur associé au groupe sélectionné.
Statuts disponibles = En service, Suspendu et Volé

« Plage d'accès »
Le menu déroulant affiche la liste de toutes les plages utilisateurs disponibles (page 71).

« Société »
Ce menu déroulant permet de définir à quelle(s) société(s) ou locataire(s) appartient le badge et l'utilisateur.

Tous les badges enrôlés via le menu « Apprentissage » intègrent la base de données principale ainsi que la liste des badges (page 76)

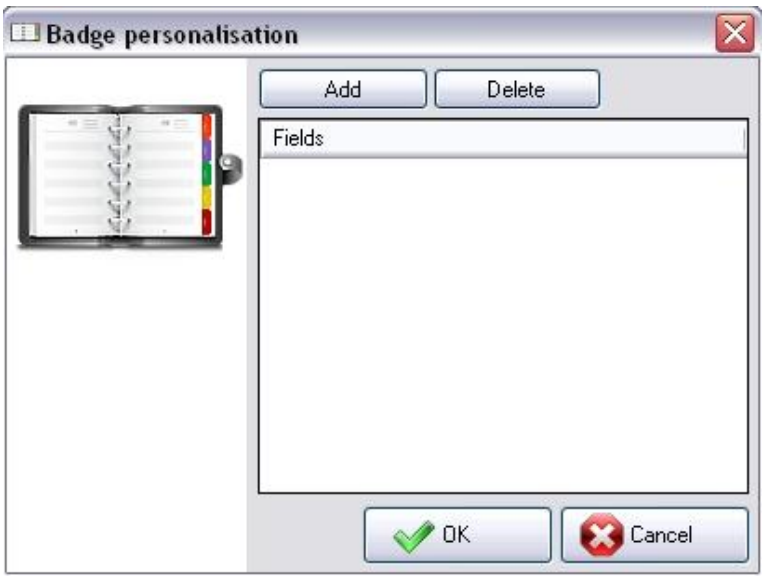
Les utilisateurs et les badges

Personnalisation du Badge

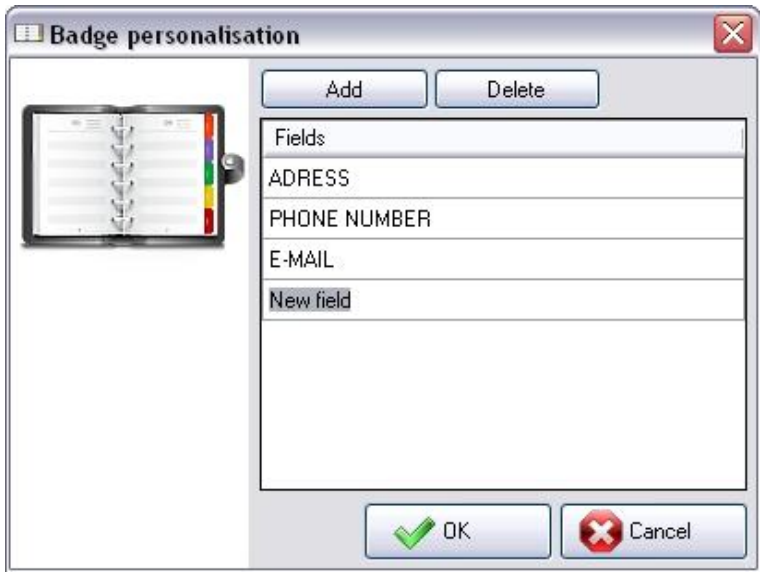
Sélectionnez Contrôle d'accès → Personnalisation des Badges

Cette fonction permet de créer et d'ajouter des champs complémentaires qui s'afficheront dans les fiches badges/utilisateurs du site.

Ces différents champs pourront être renseignés dans chaque fiche badge/utilisateur et serviront aussi comme filtre de recherche « historique » du logiciel (page 137).



« Ajouter »
Cliquez sur ce bouton pour créer un nouveau champ complémentaire.
Une nouvelle ligne apparaît dans la fenêtre principale du menu.
Double-cliquez sur cette ligne afin de modifié l'intitulée « Nouveau Champs » de base.



« Supprimer »
Sélectionnez le champs complémentaire puis cliquez sur le bouton supprimer.

La suppression de ce champ entrainera la suppression de tout le paramétrage associé

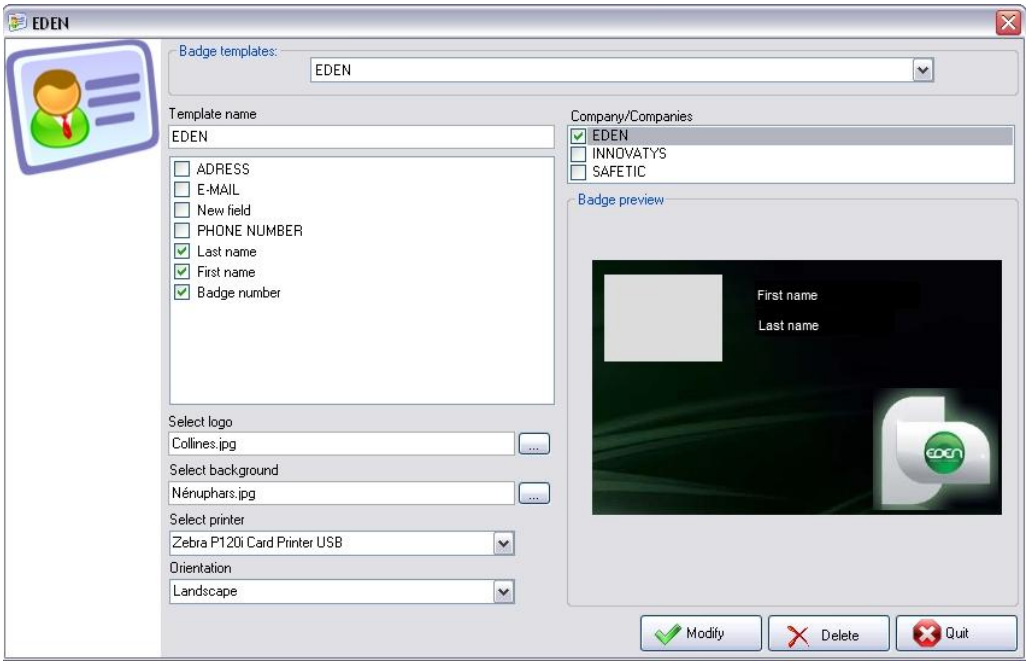
Les utilisateurs et les badges

Modèle de badge imprimable

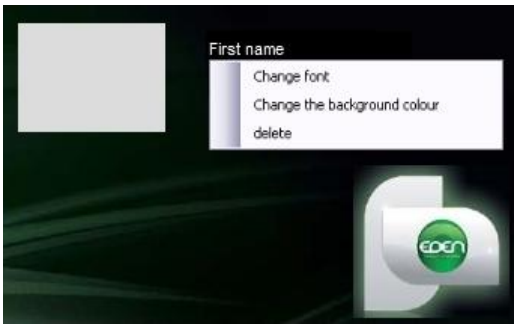
Sélectionnez Contrôle d'accès → Modèle de badge imprimable

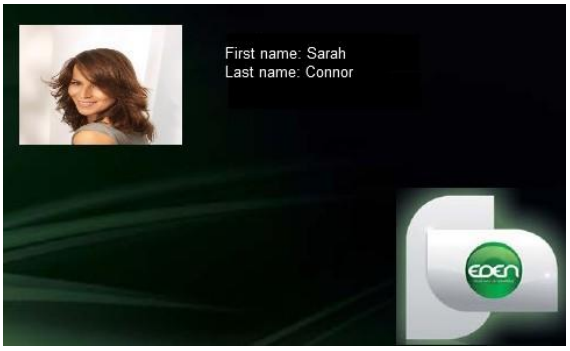
Cette fonction permet la personnalisation des badges via une imprimante thermique spécialisée du marché.
Vous pouvez créer plusieurs modèles graphiques d'impression suivant les besoins du site sans limite.
Les imprimantes du marché intégrant des drivers « Windows » sont compatibles avec ce module.

« Société »
Ce menu déroulant permet de définir à quelle société appartient le badge et l'utilisateur.



1.Éditez un intitulé dans le champ « Nom du modèle »
2. Sélectionnez et cochez les cases des informations souhaitées pour ce modèle d'impression de badges
3. Les informations sélectionnées apparaîtront dans la fenêtre de droite.
4. Il suffit ensuite de les déplacer par simple glisser-déposer
5. Vous pouvez changer la taille et la couleur de la police des caractères
6. Vous pouvez ajouter un logo et un fond d'écran
7. Sélectionnez l'imprimante
8. Choisissez l'orientation du badge au format vertical ou horizontal





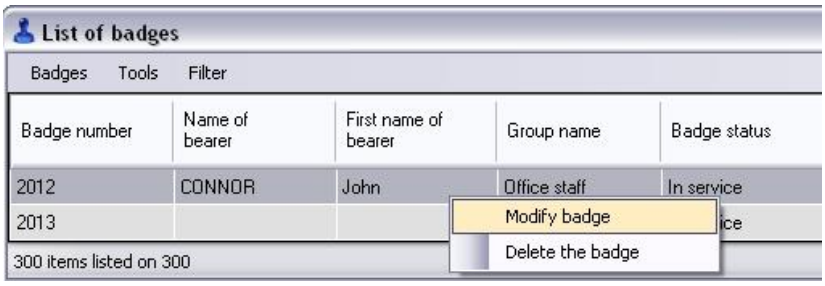
Les utilisateurs et les badges

La fiche badge/utilisateur

Sélectionnez Contrôle d'accès → Badges → Liste des badges

1. Le profil « standard »

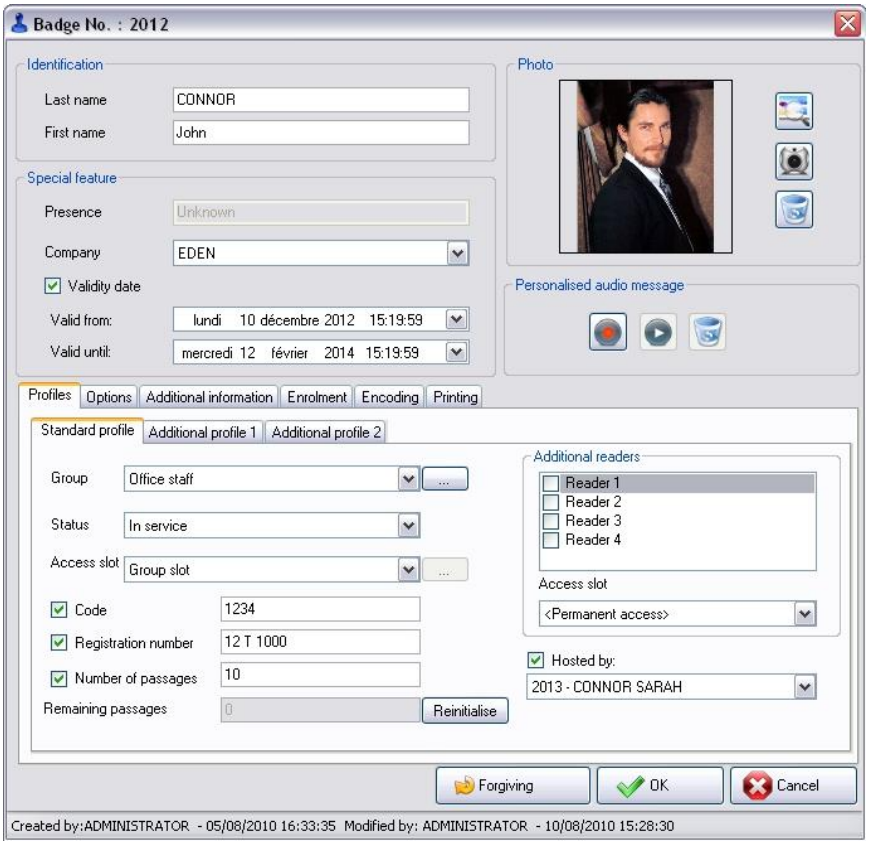
Ce menu permet de paramétrer et modifier la fiche badge d'un utilisateur. Le logiciel SENATORFX.NET peut gérer 10.000 fiches individuelles.



Double-cliquez sur la ligne du badge souhaité ou effectuez un clic-droit puis « modifier le badge »

Paramétrage de la fiche « Utilisateur »

1.Éditez le nom de l'utilisateur dans le champ « nom »
2.Éditez le prénom de l'utilisateur dans le champ « prénom »
3. Sélectionnez la société à qui il appartient dans le menu déroulant « société » (création page 95)
4. Cochez la case « date de validité » si nécessaire et éditez les dates et heures de début/fin souhaitées dans les champs correspondants
5. Vous pouvez enregistrer un son et une photo via la webcam fournie avec le logiciel.
6. **« Profil standard » :** Affectez ou modifiez le groupe d'accès de l'utilisateur via le menu déroulant ou le visualiser via le bouton « … »
7. Changez le statut du badge dans le champ « statut »
8. Plage d'accès affiche par défaut la plage du groupe. Il est possible de choisir une autre plage que la plage d'accès du groupe en la sélectionnant dans le menu déroulant.
9. Cochez la case « Code » pour affecter un code NIP
10. Cochez la case « Immatriculation » pour éditer le N° de la plaque d'immatriculation du véhicule de l'utilisateur.



11. Cochez la case « Nombre de passage » pour éditez un crédit de passage pour cet utilisateur

12. Cochez des lecteurs additionnels si vous souhaitez étendre les droits d'accès sans changer le groupe d'accès de cet utilisateur

13. Choisissez une plage horaire qui sera affectée aux lecteurs additionnels via le menu déroulant

14. Cochez la case « Accompagné par » et sélectionnez le badge accompagnateur pour activer la fonction Accompagnateur/accompagné

Les utilisateurs et les badges

La fiche badge/utilisateur

Sélectionnez Contrôle d'accès → Badges → Liste des badges

2. Les profils « additionnels »

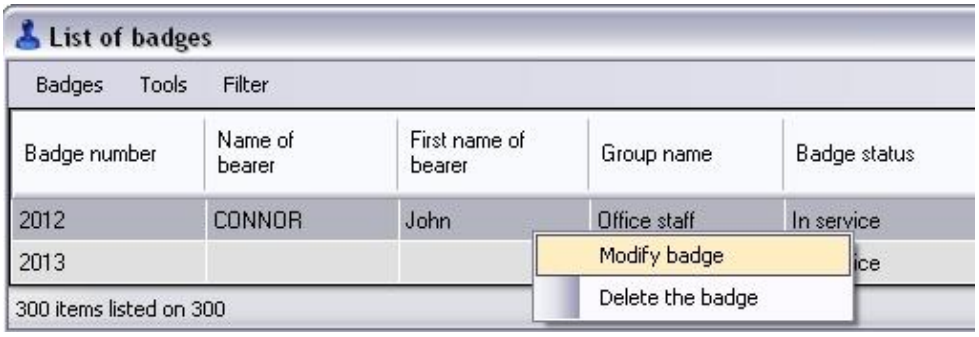
Ce menu permet de paramétrer et modifier les paramètres de l'onglet « Profils additionnels 1 et 2.
Ces profils peuvent être activés via la gestion de « **l'état de crise** » ou d'autres paramètres.

Descriptif des « Profils additionnels 1/2 »

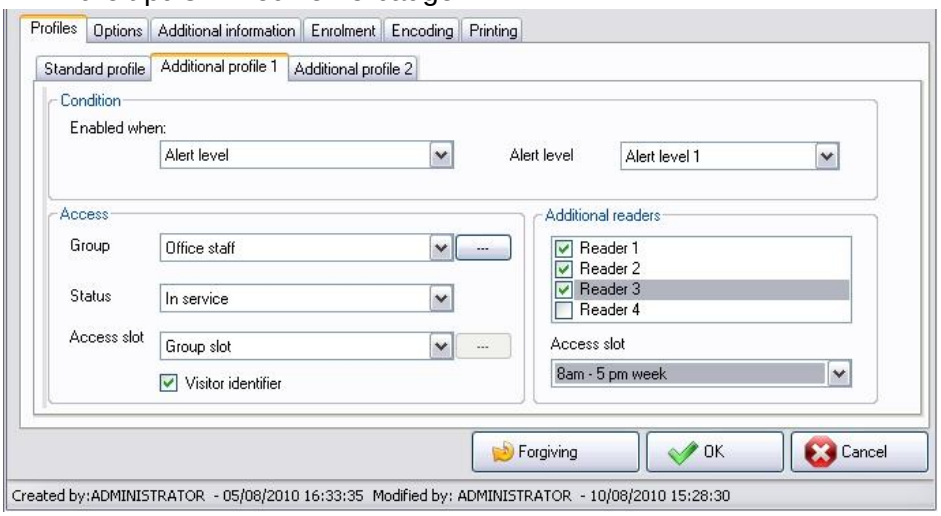
Ces profils seront activés selon des conditions décrites ci-dessous.
Deux profils ne peuvent être activés en même temps.
Sélectionnez la condition souhaitée via le menu déroulant

Les conditions disponibles

- **Jamais =** Profil jamais activé
- **Niveau d'alerte =** sélectionnez via le menu déroulant le niveau d'alerte. Les niveaux d'alerte peuvent être activés via les opérateurs du logiciel ou via des scénarios préétablis
- **Niveau d'alerte minimum** = sélectionnez via le menu déroulant le niveau d'alerte minimum requis. Les niveaux d'alerte peuvent être activés via les opérateurs du logiciel ou via des scénarios préétablis
- **Plage Auto** = sélectionnez via le menu déroulant la plage horaire qui activera ce profil lorsqu'elle sera active
- **Période** = définir la date de début /fin qui activera le profil
- **Profil permanent** = Profil toujours activé



- Double-cliquez sur la ligne du badge souhaité ou effectuez un clic-droit puis « modifier le badge »



Paramètres possibles

1. Affectez le groupe d'accès via le menu déroulant
2. Changez le statut du badge
3. Plage d'accès affiche la liste de toutes les plages horaires disponibles
4. Cochez des lecteurs additionnels si nécessaire
5. Choisissez une plage horaire qui sera affectée aux lecteurs additionnels
6. Cochez la case « identifiant accompagné » si nécessaire

Toutes ces paramètres sont identiques à ceux du profil « standard » et expliqués page 81.

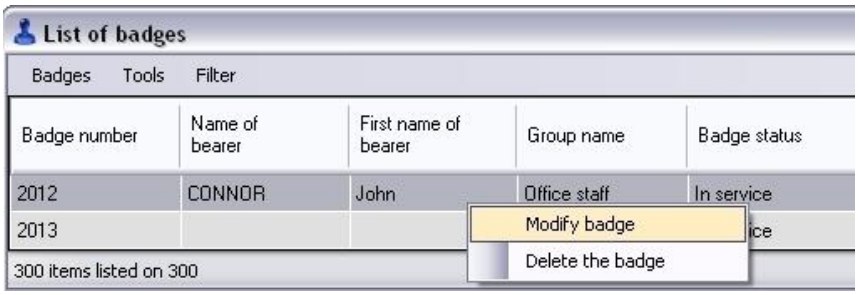
Les utilisateurs et les badges

La fiche badge/utilisateur

Sélectionnez Contrôle d'accès → Badges → Liste des badges

3. L'onglet « Options »

Ce menu permet de paramétrer et modifier les paramètres de l'onglet « Profils additionnels 1 et 2. Ces profils peuvent être activés via la gestion de « **l'état de crise** » ou d'autres paramètres.



Double-cliquez sur la ligne du badge souhaité ou effectuez un clic-droit puis « modifier le badge »

Description « Badges spéciaux »
Si la case de l'option est cochée, alors:

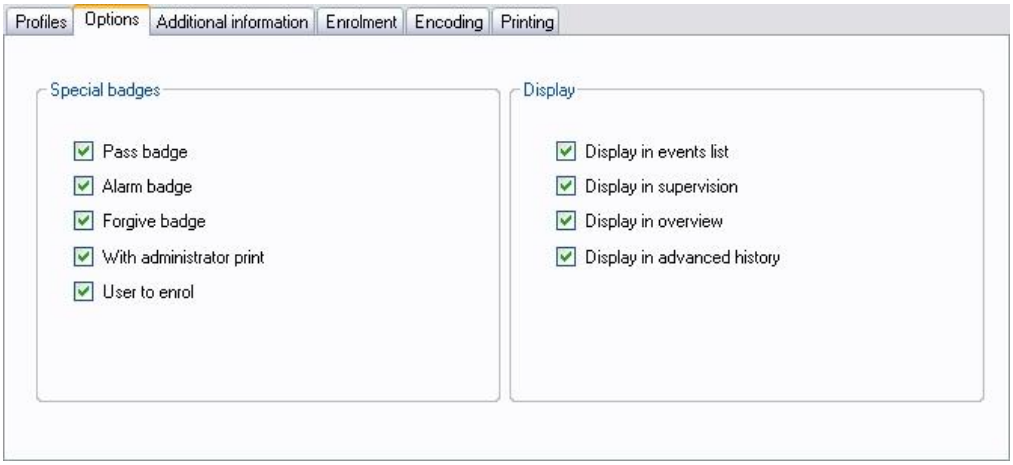
« Badge passe »
Cette fonction permet au porteur du badge de ne plus être soumis à l'anti-passback

« Badge alarme »
Ce paramètre autorise le porteur du badge à activer une sortie relais supplémentaire lors de son passage sur un lecteur autorisé. La fonction doit être activée sur les lecteurs souhaités (voir page 46)

« Badge de remise en cycle »
Il s'agit d'un badge qui effectue un RAZ de tous les badges du site

« L'administrateur »
L'administrateur est un utilisateur qui peut enrôler les empreintes biométriques des autres utilisateurs

« **Utilisateur à enrôler** »
Cela permettra de déclencher l'enrôlement des empreintes biométriques lors du passage d'un badge/utilisateur possédant le statut « administrateur »



Description « Afficher »
Si la case de l'option est cochée, alors:

« Afficher dans la liste des événements »
Chaque événement généré par le badge/utilisateur s'affichera dans le monitoring du fil de l'eau appelé « liste des événements ».

« Afficher dans la supervision»
Chaque événement généré par le badge/utilisateur s'affichera dans le menu « Supervision » des plans dynamiques.

« Afficher dans le synoptique »
Chaque événement généré par le badge/utilisateur s'affichera dans le menu « Synoptique » des plans dynamiques.

« Afficher dans l'historique avancé»
Chaque événement généré par le badge/utilisateur s'affichera dans le menu « historique avancé»

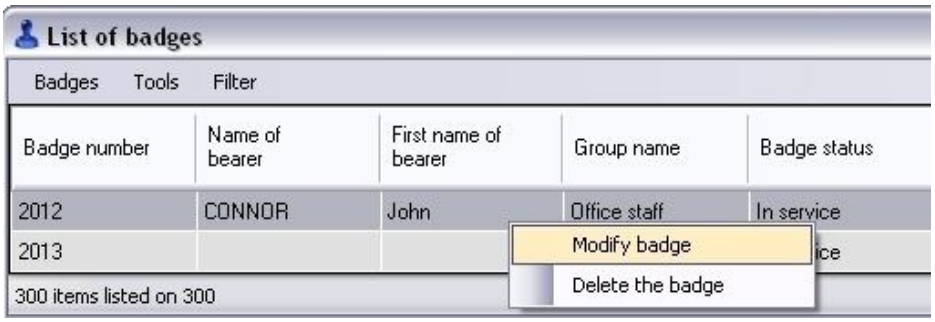
Les utilisateurs et les badges

La fiche badge/utilisateur

Sélectionnez Contrôle d'accès → Badges → Liste des badges

4. L'onglet « Informations complémentaires »

Ce menu permet d'éditer les champs complémentaires d'informations affectées aux badges et aux utilisateurs.
Ces champs complémentaires sont crées dans le menu « Personnalisation des badges ».
Le nombre de ces champs complémentaires est illimité. Ils peuvent servir de filtre pour les requêtes du menu « Historique avancé ».



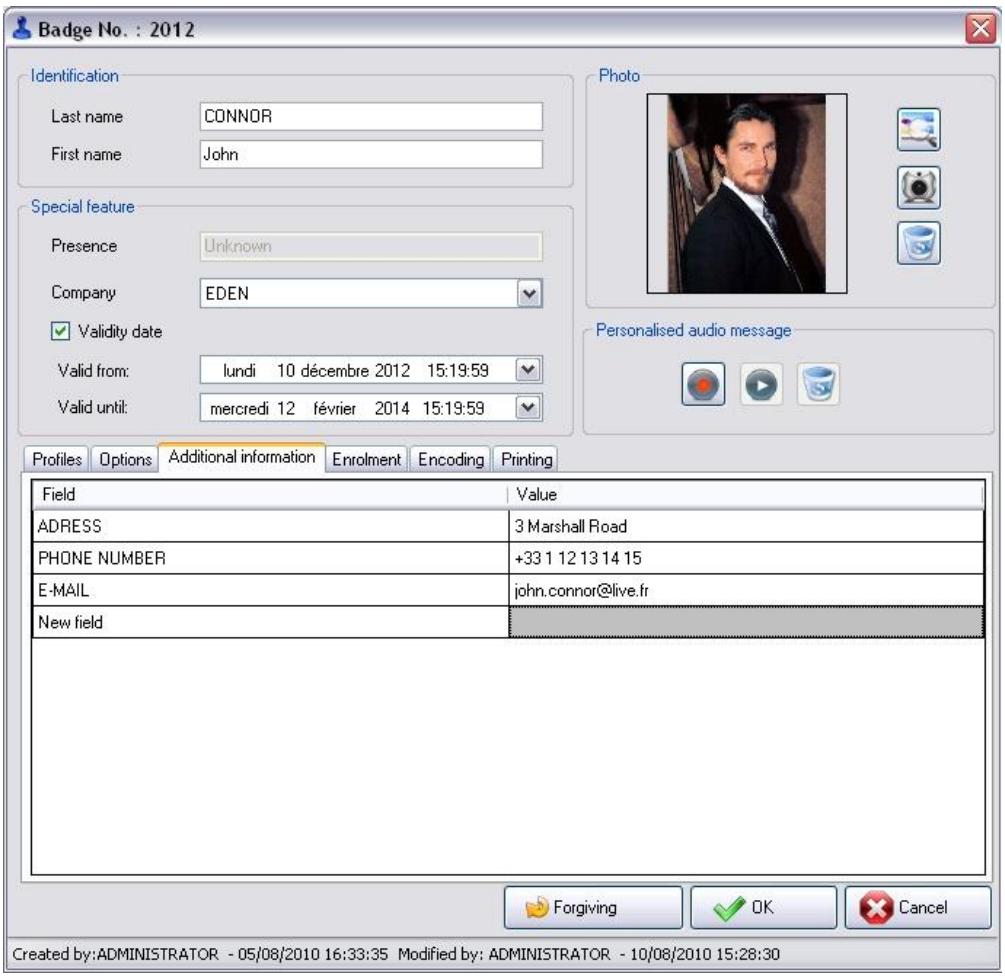
Double-cliquez sur la ligne du badge souhaité ou effectuez un clic-droit puis « modifier le badge »

Procédure

1. Sélectionnez le champ complémentaire à modifier dans la colonne « Valeur »

2. Double-cliquez sur le champ

3. Éditez le libellé souhaité



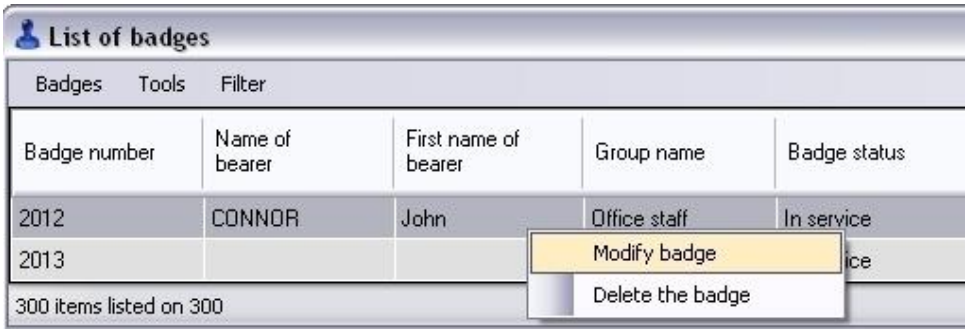
Les utilisateurs et les badges

La fiche badge/utilisateur

Sélectionnez Contrôle d'accès → Badges → Liste des badges

5. L'onglet « Enrôlement »

Cet onglet apparaît dans la fiche badge/utilisateur seulement s'il est déclaré dans le logiciel des lecteurs biométriques d'empreinte digitale « SOLO » et du réseau veineux du doigt « BIOVEIN » (page 39).Le but principal est de lancer la phase d'enrôlement des empreintes biométriques de l'utilisateur directement via sa fiche. Quelque soit la technologie biométrique utilisée, l'on peut enrôler deux empreintes par utilisateur.



Double-cliquez sur la ligne du badge souhaité ou effectuez un clic-droit puis « modifier le badge »

Procédure

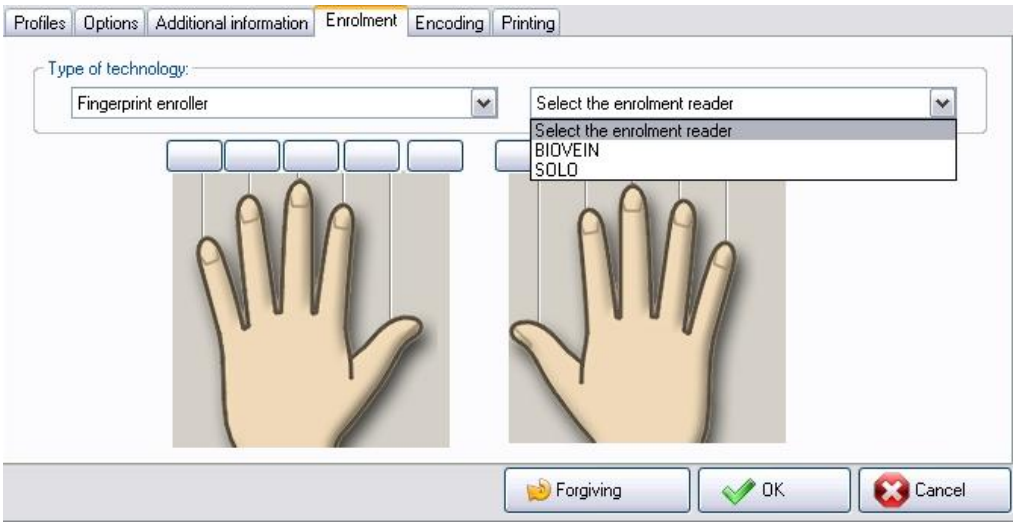
1. Sélectionnez dans le menu déroulant « Type de la technologie » la technologie souhaitée pour l'enrôlement de l'identifiant biométrique de cet utilisateur.

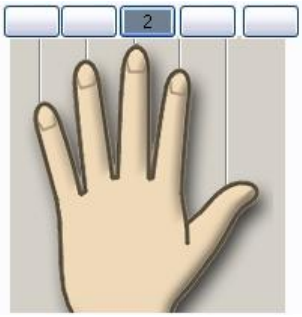
2. Dans le menu déroulant de droite choisissez le lecteur d'enrôlement des identifiants biométriques.

3. Sélection le premier doigt pour lancez la phase d'enrôlement.

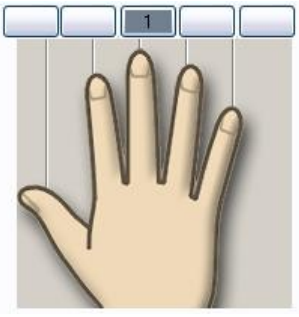
4.À l'affichage de cette nouvelle fenêtre, présentez votre doigt sur le lecteur choisi et effectuez l'enrôlement.

5. Répétez cette phase pour le second doigt si besoin.





Second doigt enregistré



Premier doigt enregistré

L'utilisation de l'empreinte digitale en France selon le texte de loi de la CNIL, les empreintes doivent être stockées dans un badge Mifare pour une utilisation en « empreinte + badge »

Les utilisateurs et les badges

La fiche badge/utilisateur

Sélectionnez Contrôle d'accès → Badges → Liste des badges

6. L'onglet « Encodage »

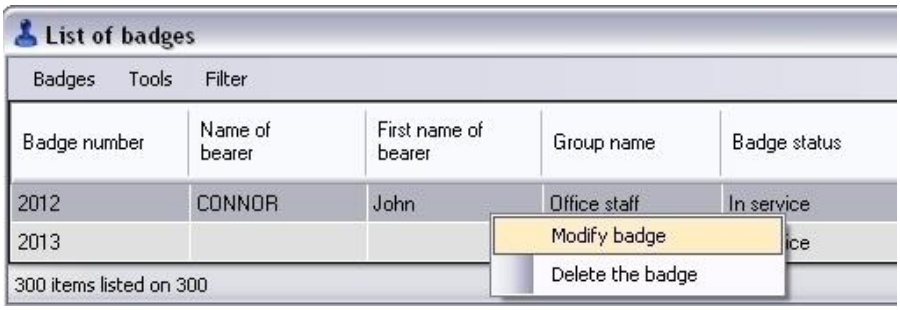
Cet onglet apparaît dans la fiche badge/utilisateur seulement s'il est déclaré dans le logiciel un module d'encodage de badge Mifare « ENCODUSB » (page 30).
Cet onglet permet d'encoder les empreintes digitales précédemment enrôlées (page 77) dans un badge Mifare.
Cela permet de répondre aux préconisations de la CNIL en France avec l'utilisation des empreintes digitale.
L'on pourra donc après cet encodage, utilisé la fonction « Empreinte + badge » ou « badge sans empreinte ».

Actions possibles

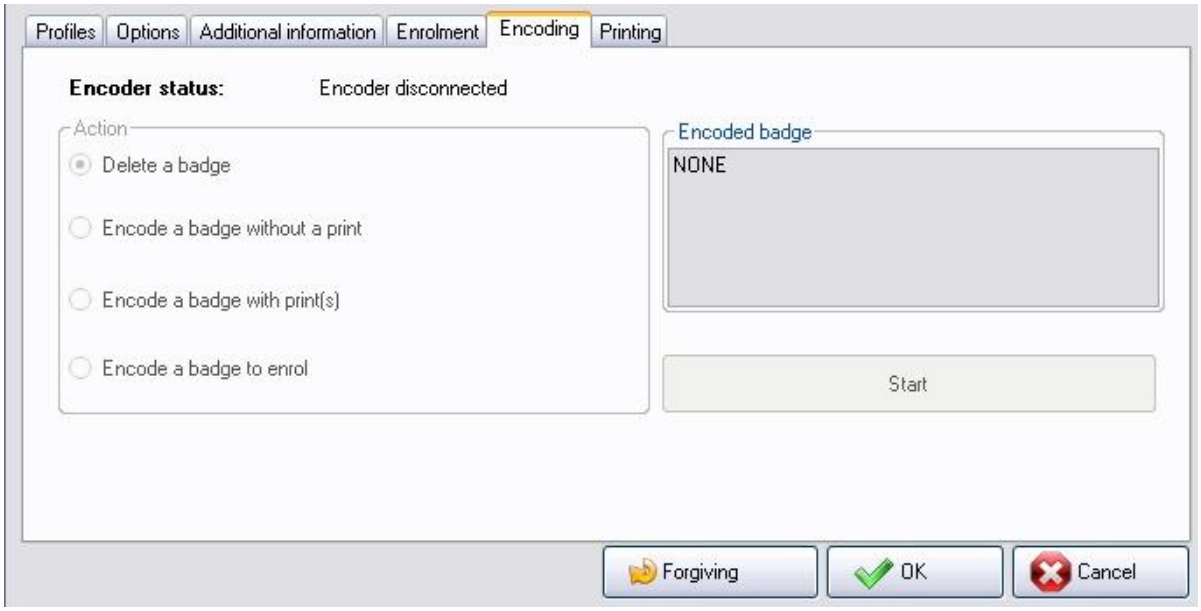
« Effacer un badge »
Effacement des informations contenues dans les 16 premiers secteurs du badge Mifare présent sur l'encodeur « **ENCODUSB** ».

« Badge sans empreinte »
Cette fonction déclenche l'encodage du badge lorsqu'il est sélectionné. Cela peut être utile pour les personnes ne possédant pas d'empreinte. Il faudra toutefois autoriser les badges sans empreintes dans la configuration des lecteurs (page 46).

« Badge avec empreinte »
Lorsqu'il est sélectionné, déclenche l'enrôlement du doigt et l'encodage du badge, si un encodeur et un enrôleur USB sont déclarés. Si seulement un encodeur est déclaré, le bouton « Badge avec empreinte » fonctionnera de la même façon que le bouton « badge à enrôler ».



Double-cliquez sur la ligne du badge souhaité ou effectuez un clic-droit puis « modifier le badge »



« Badge à enrôler »
Lorsqu'il est sélectionné déclenche l'encodage du badge. Une fois le badge encodé il suffira pour déclencher l'enrôlement, de présenter le badge devant un des lecteurs biométrique de l'installation. Il faut, lorsque le lecteur émet des bips présenter 3 fois un doigt. Une fois l'enrôlement terminé, il faut représenter le badge devant le lecteur pour que ce dernier reçoive l'empreinte.

Uniquement les badges Mifare 1K sont compatibles avec l'ENCOD-USB. La référence EDEN est « MA8000 ».

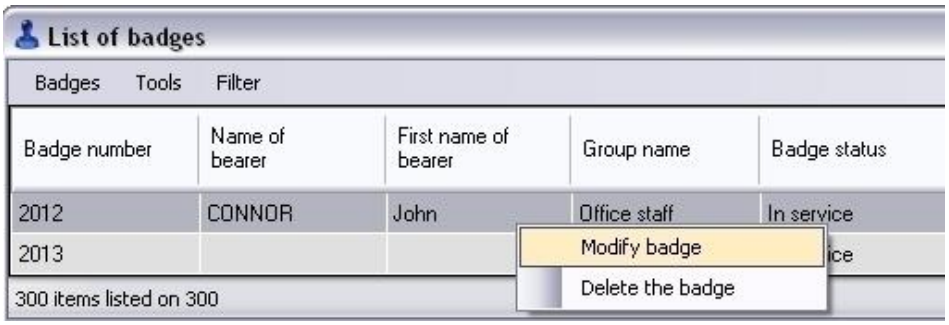
Les utilisateurs et les badges

La fiche badge/utilisateur

Sélectionnez Contrôle d'accès → Badges → Liste des badges

7. L'onglet « Impression »

Cet onglet apparaît dans la fiche badge/Utilisateur seulement s'il est déclaré un « modèle de badge imprimable » expliqué page 72.
Cet onglet permet d'imprimer un badge suivant un modèle préétabli avec les paramètres de cet utilisateur.



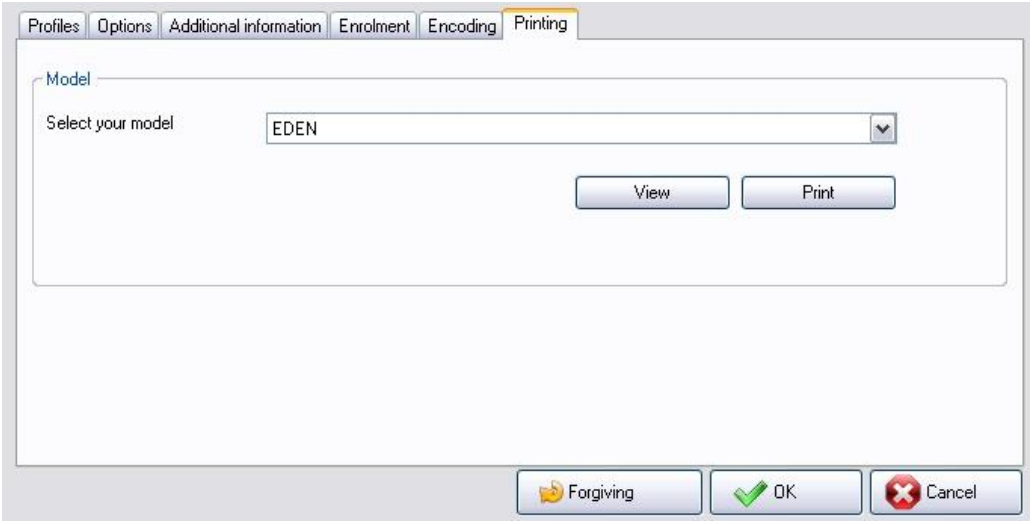
Double-cliquez sur la ligne du badge souhaité ou effectuez un clic-droit puis « modifier le badge »

Procédure

1. Sélectionnez dans le menu déroulant le modèle d'impression préétabli dans le menu

2. Si vous souhaitez voir le modèle d'impression, cliquez sur le bouton « Visualiser »

3. Si vous souhaitez imprimer le badge suivant le modèle d'impression choisi, cliquez sur le bouton « Imprimer »



Fenêtre d'aperçu du modèle d'impression choisi avec les informations de l'utilisateur.

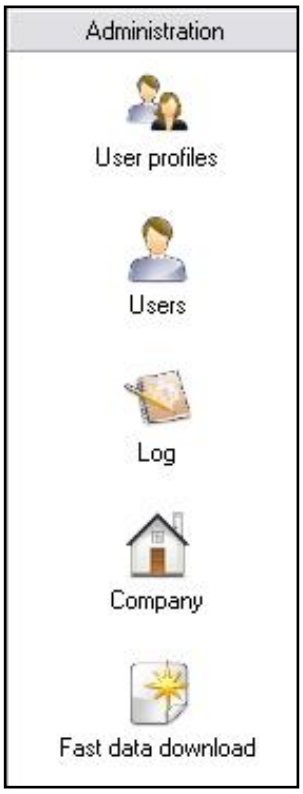
Les utilisateurs et les badges

La fiche badge/utilisateur

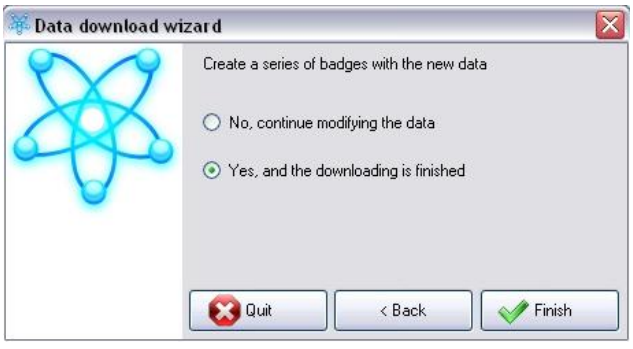
8. Récupération rapide des données

Sélectionnez l'onglet « Administration » → Récupération rapide des données

La « Récupération rapide des données » permet d'importer une base de données externe sous forme de tableur.
L'on peut importer les champs disponibles de la fiche badge/utilisateur et affecter un droit d'accès et un N° de badge.



Data download wizard
Preparing the data recovery
1 : Open the document containing the data to recover using its application (eg: xls file with Excel
2 : Copy all the data to be recovered to the clipboard
(Select it then Menu Edit->Copy or Ctrl+C)
Quit
Next >



Procédure

1. Cliquez sur « Récupération rapide des données ».

2. Ouvrez le document de type tableur contenant les données à importer dans le logiciel SENATORFX.NET.

3. Sélectionnez et copiez les données à importer dans le « presse-papier » de Windows.

4. Cliquez sur le bouton « suivant » de l'assistant de récupération des données
5. Via un menu déroulant, L'assistant vous propose pour chaque type de données la liste des champs disponibles dans les fiches badges/Utilisateurs.

6. Choisissez un champs pour chaque type de donnés à importer

7. Afin d'optimiser l'importation, il faut créer une série de badges à affecter aux données importées.

8.Éditez le N° du premier badge à affecter pour cette nouvelle série.

9.Éditez les paramètres proposés comme à la page 69, puis validez par le bouton « OK ».

10. Cette nouvelle série de badge/utilisateurs s'affichera alors dans la liste des badges comme à la page 69

Chapitre 6

Les opérateurs du logiciel

Que contient ce chapitre ?

Les opérateurs du logiciel 88
Les profils des opérateurs 89
1.Créer un Profil 89
Les profils des opérateurs 90
2.Modifiez un Profil 90
3.Supprimer un profil 90
Les opérateurs 91
1.Créer un Opérateur 91
Les opérateurs 92
2.Modifier un Opérateur 92
3.Supprimer un Opérateur 92
Le journal de bord 93
Gestion Multi-société/Locataires 94

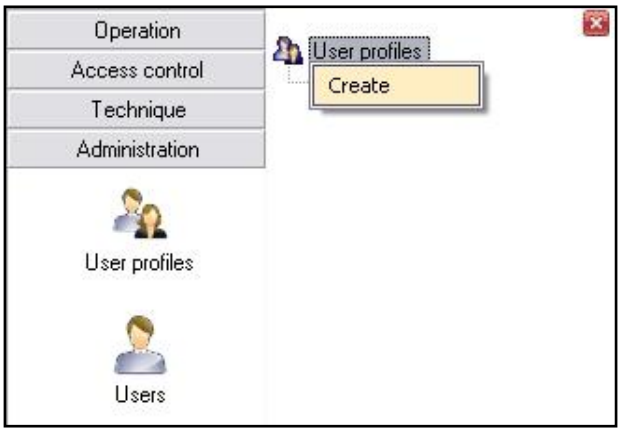
Les opérateurs du logiciel

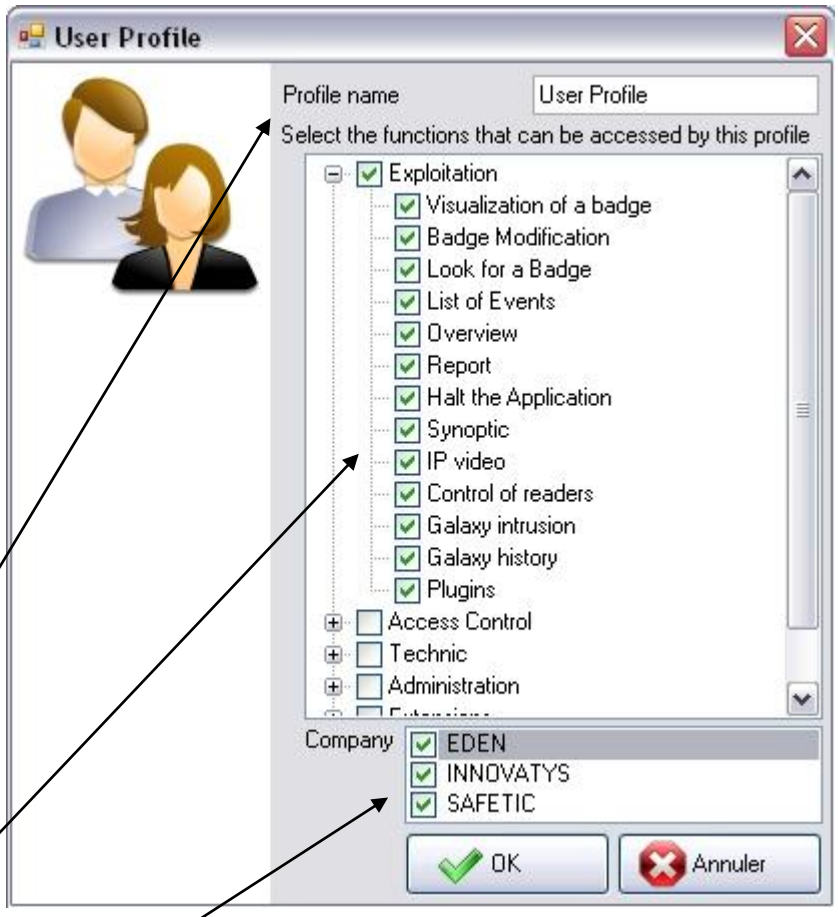
Les profils des opérateurs

Sélectionnez « Administration » → Profils d'utilisateur → Créer un profil

1. Créer un Profil

Ce menu permet la création des droits d'accès des opérateurs du logiciel SENATORFX.NET à partir de filtres entièrement paramétrables par le gestionnaire du site.
Un profil pet être associé à un ou plusieurs opérateurs du logiciel suivant les besoins de gestion du site.
Vous pouvez créer autant de profils d'opérateurs que vous le souhaitez.





- Sélectionnez « Profils d'utilisateur »
- « Créer un profil »

Procédure

1.Éditez un nom pour le profil en cours dans le champ « Nom du profil ».Ce libellé s'affichera dans tout le logiciel.

2.Cochez les cases correspondantes des menus et sous-menus que vous souhaitez afficher lors de l'utilisation du logiciel avec ce « profil Opérateur ».

3. Cochez la ou les cases des sociétés ou locataires affectées à ce « Profil Opérateur ». Il est possible que ce profil appartienne à plusieurs sociétés ou locataires du site.

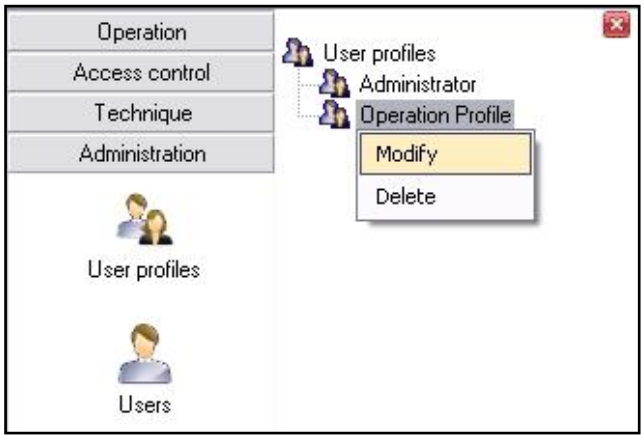
Lorsque vous créez un nouveau profil, un opérateur du nom du profil est créé et ce profil lui est affecté systématiquement.
Pour créer un nouvel opérateur du logiciel, rendez-vous dans page 83

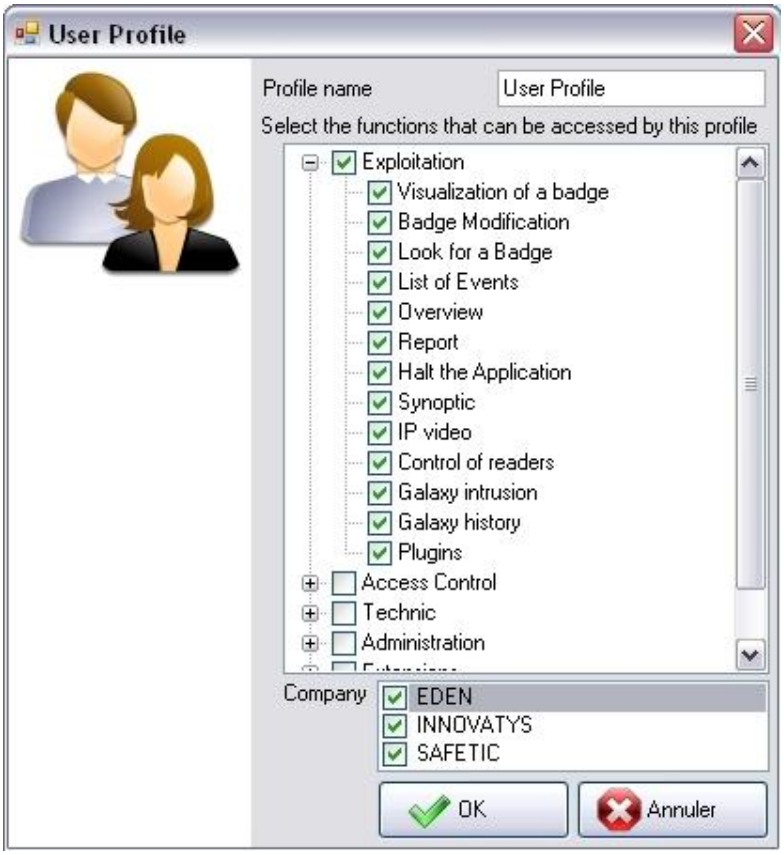
Les opérateurs du logiciel

Les profils des opérateurs

Sélectionnez « Administration » → Profils d'utilisateur

2. Modifiez un Profil

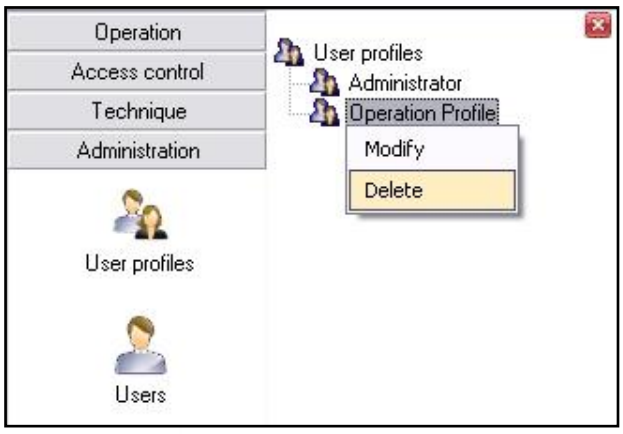


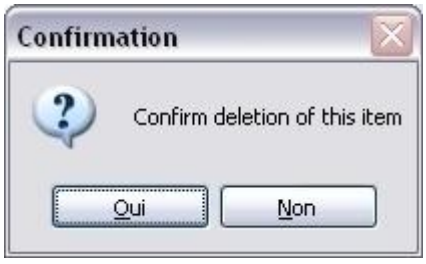


- Sélectionnez le profil souhaité
- Puis cliquez sur « Modifier »

Vous pouvez modifier tous les paramètres disponibles du profil expliqués page 82.
Les nouveaux paramètres seront appliqués à tous les opérateurs affectés à ce profil.

3. Supprimer un profil





La suppression de la fiche entrainera la suppression de tout le paramétrage associé

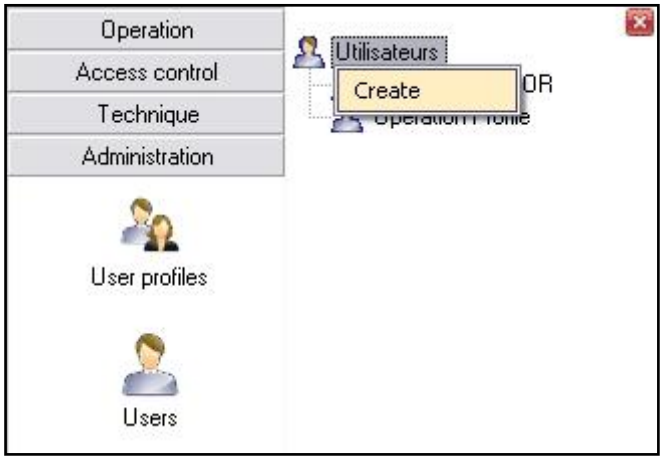
Les opérateurs du logiciel

Les opérateurs

Sélectionnez Administration → Utilisateurs

1. Créer un Opérateur

Ce menu permet la création des opérateurs/utilisateurs du logiciel SENATORFX.NET.Chaque opérateur/utilisateur est associé à un profil opérateur.
Plusieurs opérateurs/utilisateurs peuvent être associés au même profil.
Vous pouvez créer autant de fiches « opérateur/utilisateur » que vous le souhaitez.



- Cliquez sur « Utilisateur »
- Sélectionnez « Créer un utilisateur »

Procédure

1. Éditez un nom pour l'opérateur dans le champs « Nom ».
2. Éditez un prénom pour l'opérateur dans le champs « Prénom ».
3. Sélectionnez dans le menu déroulant « profil » le profil à affecter
4. Éditez le mot de passe pour cet opérateur.
5. Confirmez le mot de passe.

Le mot de passe peut contenir tous les caractères. Il est limité à 32 caractères.

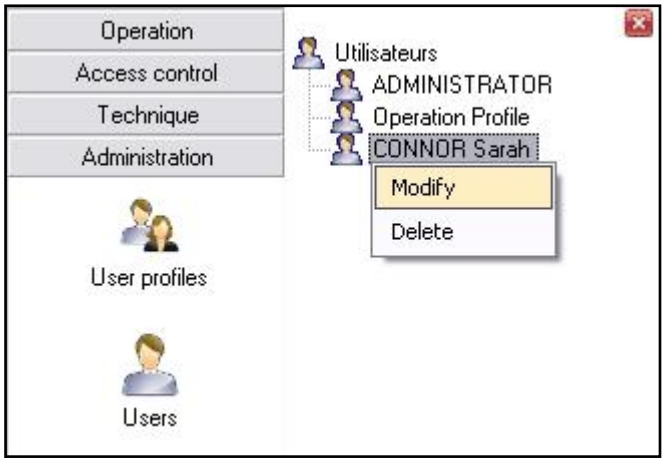
Par défaut, il existe un « opérateur Administrateur »
Afin de faciliter le premier démarrage du logiciel SENATORFX.NET, son profil ne possède pas de mot de passe.
Le profil « opérateur Administrateur » ne peut être changé.
Tous les autres paramètres peuvent être renseignés.
L'administrateur du logiciel aura accès à tous les menus ainsi qu'à toutes les sociétés.

Les opérateurs du logiciel

Les opérateurs

Sélectionnez Administration → Utilisateurs

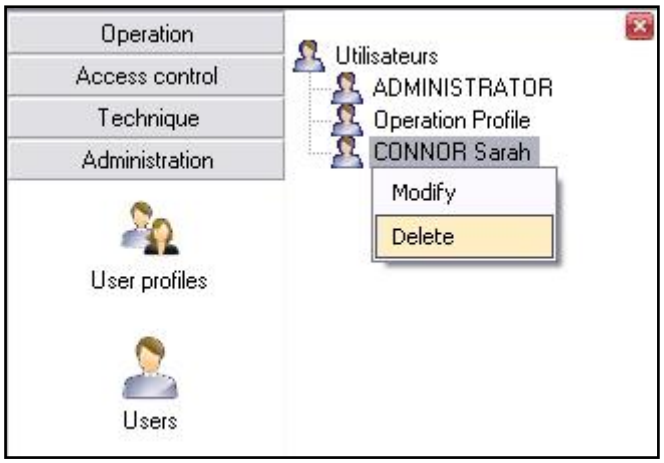
2. Modifier un Opérateur

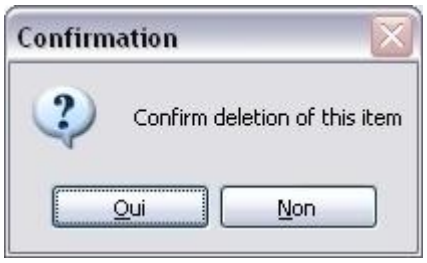


Vous pouvez modifiez tous les paramètres disponibles de l'utilisateur expliqués page 84.
Les nouveaux paramètres seront appliqués à cet opérateur

- Cliquez l »utilisateur souhaité
- Puis sélectionnez « Modifier »

3. Supprimer un Opérateur





La suppression de cet élément entrainera la suppression de tout le paramétrage associé

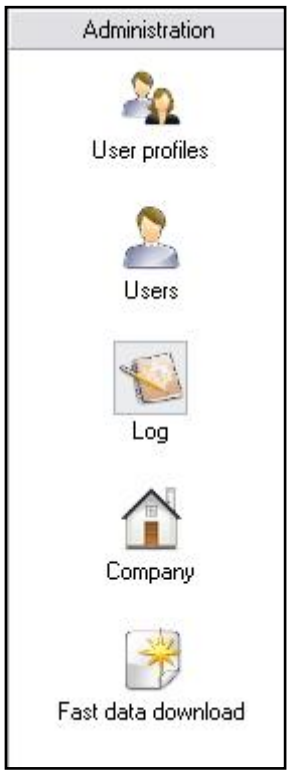
Les opérateurs du logiciel

Le journal de bord

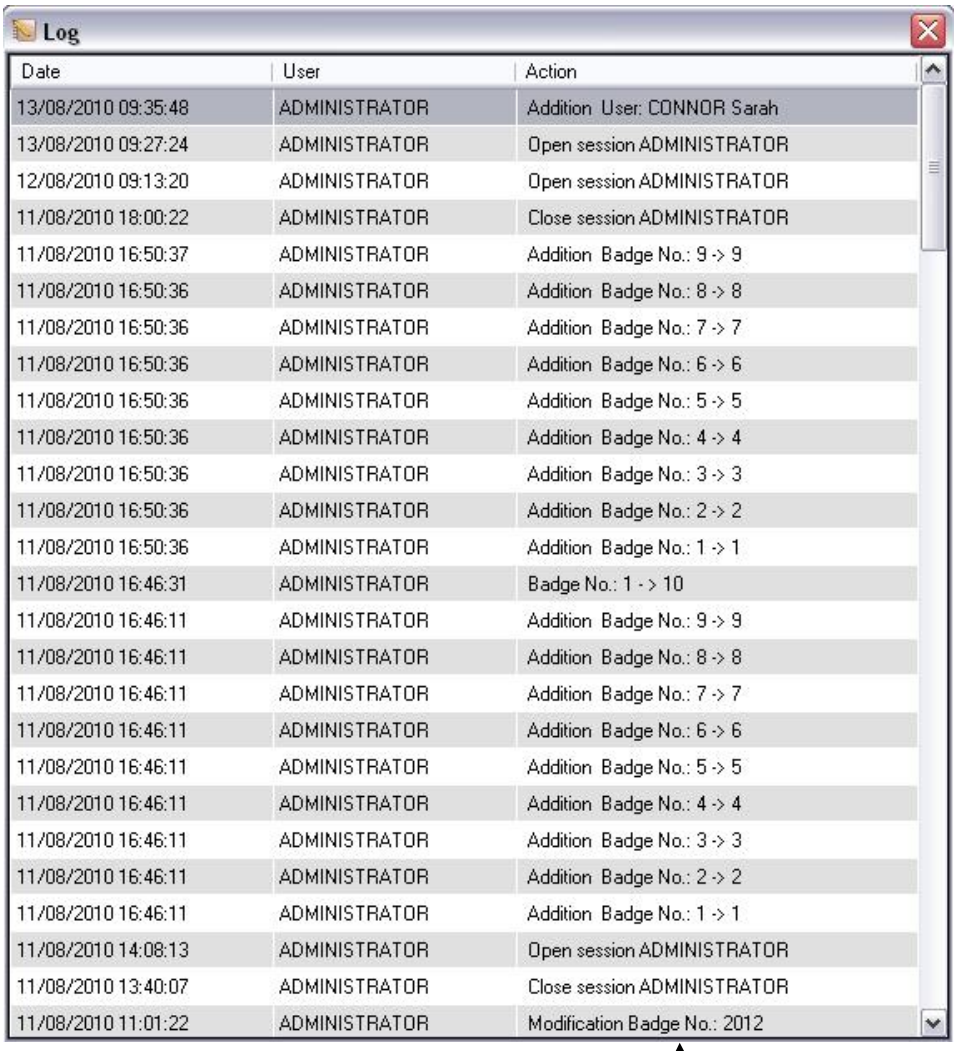
Sélectionnez Administration → Journal de bord

Le "Journal de bord" est un historique des actions qui ont été appliquées sur le logiciel par les opérateurs/utilisateurs.

Le "Journal de bord" se présente sous la forme d'un tableau à trois colonnes.
- La première colonne indique la date et l'heure de la modification.
- La seconde colonne indique le nom de l'utilisateur qui a procédé à la modification.
- La dernière colonne indique l'action qui a été effectuée par l'opérateur/utilisateur dans le logiciel.



Cliquez sur « Journal de bord»


Log
Date
User
Action
13/08/2010 09:35:48 ADMINISTRATOR Addition User: CONNOR Sarah
13/08/2010 09:27:24 ADMINISTRATOR Open session ADMINISTRATOR
12/08/2010 09:13:20 ADMINISTRATOR Open session ADMINISTRATOR
11/08/2010 18:00:22 ADMINISTRATOR Close session ADMINISTRATOR
11/08/2010 16:50:37 ADMINISTRATOR Addition Badge No.: 9 -> 9
11/08/2010 16:50:36 ADMINISTRATOR Addition Badge No.: 8 -> 8
11/08/2010 16:50:36 ADMINISTRATOR Addition Badge No.: 7 -> 7
11/08/2010 16:50:36 ADMINISTRATOR Addition Badge No.: 6 -> 6
11/08/2010 16:50:36 ADMINISTRATOR Addition Badge No.: 5 -> 5
11/08/2010 16:50:36 ADMINISTRATOR Addition Badge No.: 4 -> 4
11/08/2010 16:50:36 ADMINISTRATOR Addition Badge No.: 3 -> 3
11/08/2010 16:50:36 ADMINISTRATOR Addition Badge No.: 2 -> 2
11/08/2010 16:50:36 ADMINISTRATOR Addition Badge No.: 1 -> 1
11/08/2010 16:46:31 ADMINISTRATOR Badge No.: 1 -> 10
11/08/2010 16:46:11 ADMINISTRATOR Addition Badge No.: 9 -> 9
11/08/2010 16:46:11 ADMINISTRATOR Addition Badge No.: 8 -> 8
11/08/2010 16:46:11 ADMINISTRATOR Addition Badge No.: 7 -> 7
11/08/2010 16:46:11 ADMINISTRATOR Addition Badge No.: 6 -> 6
11/08/2010 16:46:11 ADMINISTRATOR Addition Badge No.: 5 -> 5
11/08/2010 16:46:11 ADMINISTRATOR Addition Badge No.: 4 -> 4
11/08/2010 16:46:11 ADMINISTRATOR Addition Badge No.: 3 -> 3
11/08/2010 16:46:11 ADMINISTRATOR Addition Badge No.: 2 -> 2
11/08/2010 16:46:11 ADMINISTRATOR Addition Badge No.: 1 -> 1
11/08/2010 14:08:13 ADMINISTRATOR Open session ADMINISTRATOR
11/08/2010 13:40:07 ADMINISTRATOR Close session ADMINISTRATOR
11/08/2010 11:01:22 ADMINISTRATOR Modification Badge No.: 2012

Colonne indiquant la date et l'heure de la modification.

Colonne indiquant le nom de l'Opérateur/Utilisateur qui a procédé à la modification.

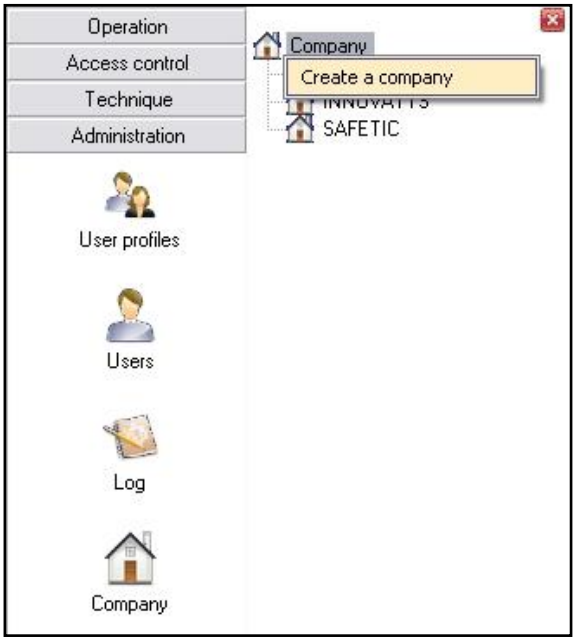
Colonne indiquant l'action qui a été effectuée par l'opérateur/utilisateur dans le logiciel.

Les opérateurs du logiciel

Gestion Multi-société/Locataires

Sélectionnez Administration → Société

La présence sur le site de plusieurs sociétés ou locataires est gérée par les affectations liées aux opérateurs/utilisateurs du logiciel SENATORFX.NET.
Chaque opérateur peut ainsi être affecté à une ou plusieurs sociétés et ne pourra pas visualiser, modifier ou gérer les autres.
Ainsi, avec seule et même base de données, via les profils des opérateurs et à partir des postes clients, chaque société ou locataire pourra manager son environnement indépendamment des autres sociétés.
Il est possible de définir certains accès « commun » qui seront gérés via un opérateur avec profil « administrateur ».
Par défaut, il n'existe qu'une seule société nommée "Default".
Il est possible de la renommer et d'en créer autant que nécessaire et cela sans limitation.



Procédé

1. Éditez un nom pour la société ou le locataire. C'est ce nom qui s'affichera dans tous les menus du logiciel ou la gestion Multi-sociétés apparaît.
2. Validez par le bouton « OK »
3. Recommencez pour les autres sociétés

- Cliquez sur « Société»
- Sélectionnez « Créer une Société »

Certains éléments peuvent appartenir à plusieurs sociétés, comme c'est le cas pour un lecteur d'entrée commune par exemple.
Le filtrage par société peut s'appliquer aux éléments suivants :
Automatisme : peut être affecté à une ou plusieurs sociétés.
Badges : ne peut être affecté qu'à une seule société.
Carte entrées/Carte sorties : peut être affecté à une ou plusieurs sociétés.
Compteurs globaux : peut être affecté à une ou plusieurs sociétés.
Consigne : peut être affecté à une ou plusieurs sociétés.
Email : peut être affecté à une ou plusieurs sociétés.
Groupe : ne peut être affecté qu'à une seule société.
Groupe d'entrées/Groupe de sorties : peut être affecté à une ou plusieurs sociétés.
Lecteur : peut être affecté à une ou plusieurs sociétés.
Liste : peut être affecté à une ou plusieurs sociétés.
Paramétrage des événements : peut être affecté à une ou plusieurs sociétés.
Plages horaires : peut être affecté à une ou plusieurs sociétés.
Profil d'utilisateurs : peut être affecté à une ou plusieurs sociétés.
Zone contrôlés : peut être affecté à une ou plusieurs sociétés.

Chapitre 7

Les extensions « logiciel »

Que contient ce chapitre ?

Les extensions « logiciel » 95
« Codes site » et « codes distributeur » 96
Préférences d'affichage 97
Gestion des Plugins 98
Gestion des fichiers XML 99
Activation de la gestion des caméras IP 101
Activation de la gestion des centrales d'alarme GALAXY 102
Rapport de configuration 103

Les extensions « logiciel »

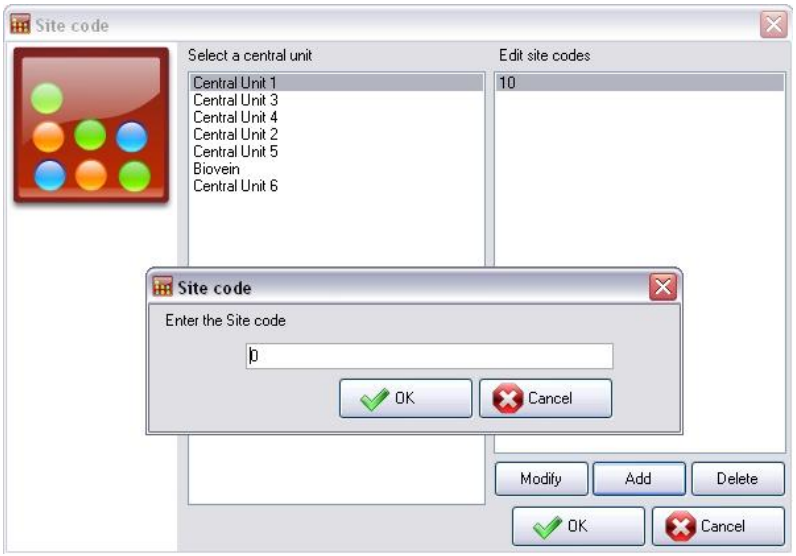
« Codes site » et « codes distributeur »

Sélectionnez extensions → « Code site »/ « Code Distributeur »

L'attribution de « Code Site » permet un niveau de sécurité supplémentaire par rapport à un site qui n'utiliserait que le numéro des badges pour l'identification des utilisateurs.
En effet lorsqu'une installation utilise les codes sites, le système contrôle dans un premier temps le code site des badges pour savoir si le badge provient bien du site, puis il contrôle le numéro du badge pour l'identification individuelle de la personne.

Gestion des « Codes Site »

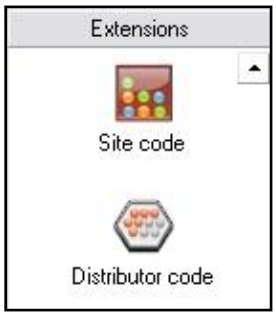
- Cliquez sur « Code Site »

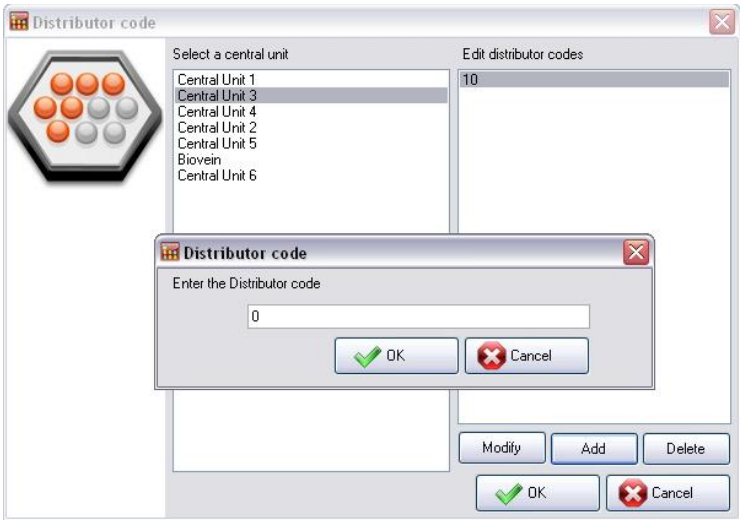


Le code site est configurable pour chaque centrale, ainsi lors de l'utilisation de la gestion multi-sociétés, il sera possible de définir un code site pour chaque société. Plusieurs codes site sont configurables sur chaque centrale, lors de l'utilisation du multi-sociétés, les accès communs auront les codes sites de toutes les sociétés crées. La liste « Sélection de la centrale » permet de sélectionner la centrale sur laquelle l'utilisateur souhaite agir sur le code site. La liste « Éditer les codes site » permet l'ajout, la modification, et la suppression des codes site de la centrale, respectivement avec les boutons « Ajouter », « Modifier » et « Supprimer ».

Gestion des « Codes Distributeur »

- Cliquez sur « Code Distributeur »





Le « Code Distributeur » offre un niveau de sécurité supplémentaire pour l'identification des badges.
Lors de l'utilisation du code distributeur, le système effectue un contrôle du code distributeur, puis du code site (si activé) puis du numéro du badge.

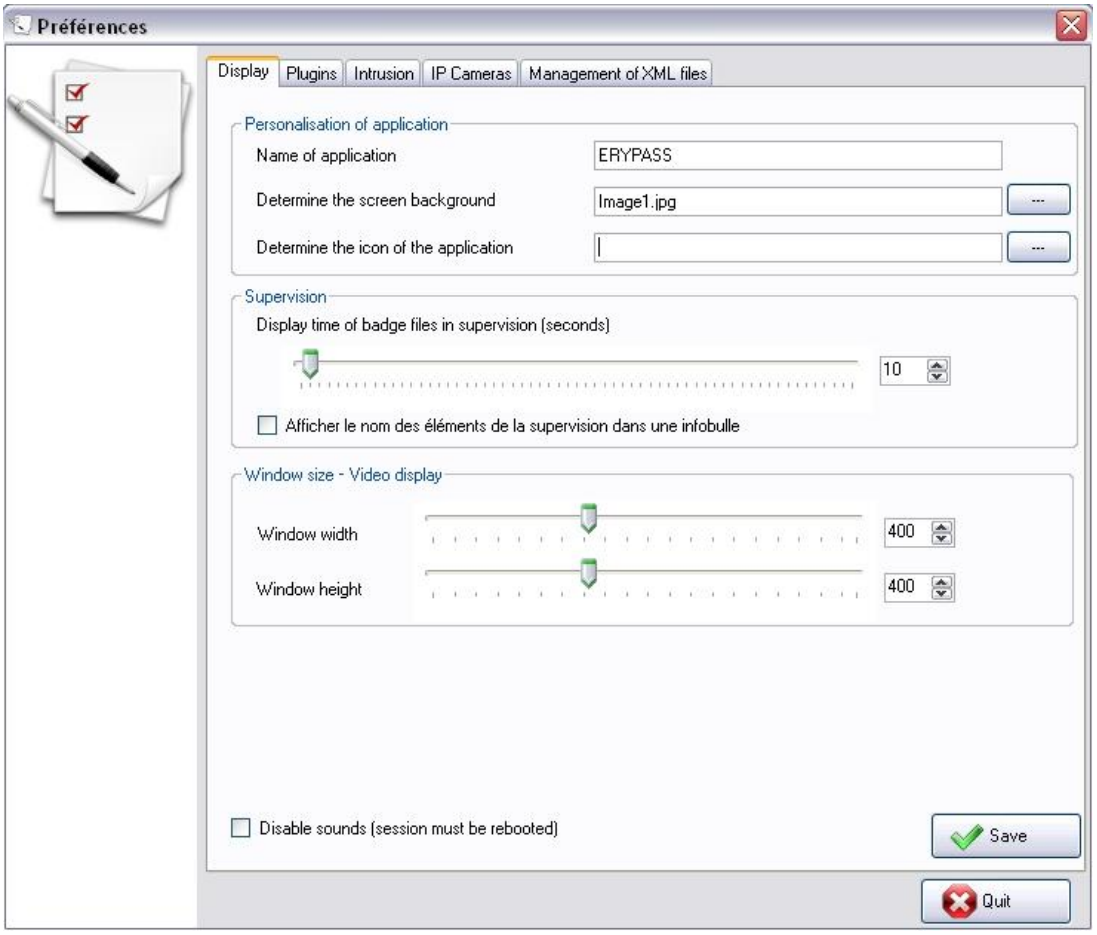
Les extensions « logiciel »

Préférences d'affichage

Sélectionnez extensions → Préférences

Ce menu permet de régler plusieurs paramètres d'affichage dans le logiciel **SENATORFX.NET**.

- Sélectionnez l'onglet « Affichage »



Nom de l'application
Édite le nom du logiciel qui s'affiche dans la barre de titre.

Déterminer le fond d'écran
Modifie le fond d'écran du logiciel.
Indique le chemin du nouveau fond d'écran.

Déterminer l'icone de l'application
Indique le répertoire où se trouve-le nouvel icône du logiciel qui s'affiche dans la barre de titre.

Durée d'affichage des fiches de badge en supervision
Règle la durée d'affichage des fiches badges lors du passage d'un badge sur un lecteur dans le menu « supervision ».

Taille des fenêtres
lorsqu'une vidéo s'affiche, représente la taille par défaut de la fenêtre qui contiendra la vidéo.

Paramétrage vidéo
Règle le temps d'un enregistrement vidéo déclenché par un automatisme.

Désactiver les sons
Active ou désactive ou les sons du logiciel (nécessite de redémarrer le logiciel).

Les extensions « logiciel »

Gestion des Plugins

Ce menu permet d'activer les modules « Plugins » optionnels dans le logiciel **SENATORFX.NET**.
Les plugins permettent d'ajouter de nouvelles fonctionnalités spécifiques au logiciel.

Sélectionnez Onglet «Plugins»

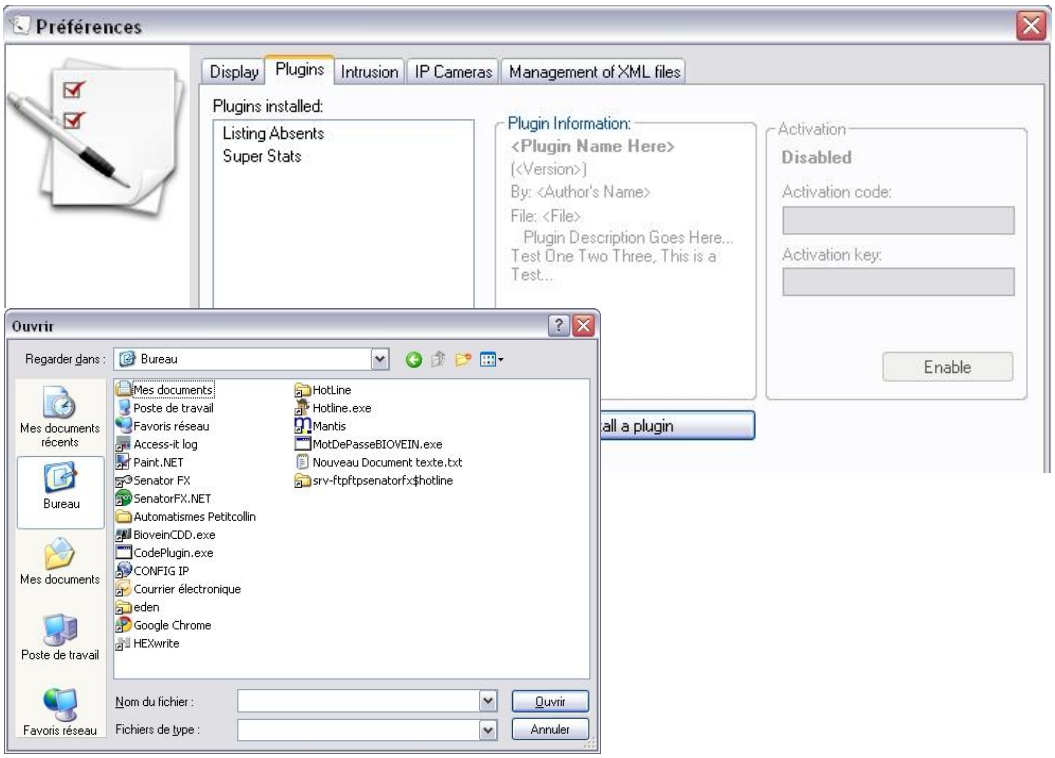
Procédure

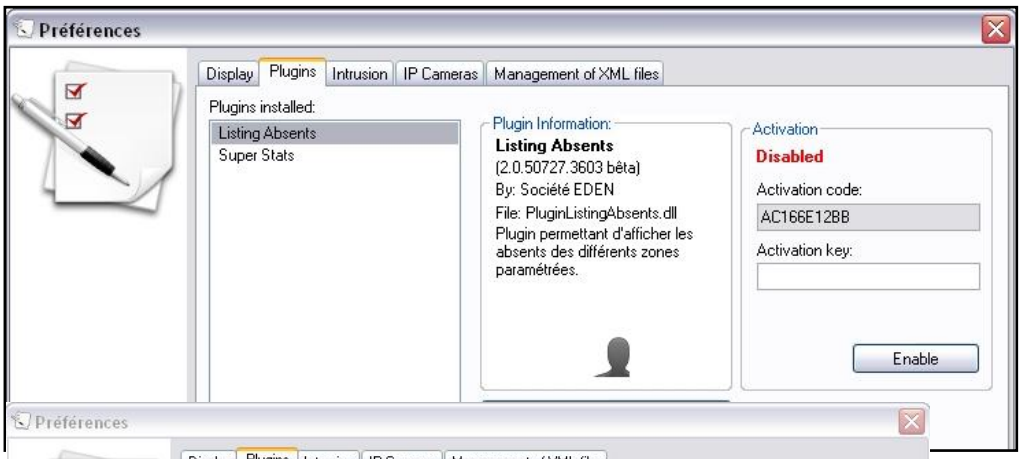
1. Pour installer un nouveau plugin, cliquez sur "Installer un plugin".

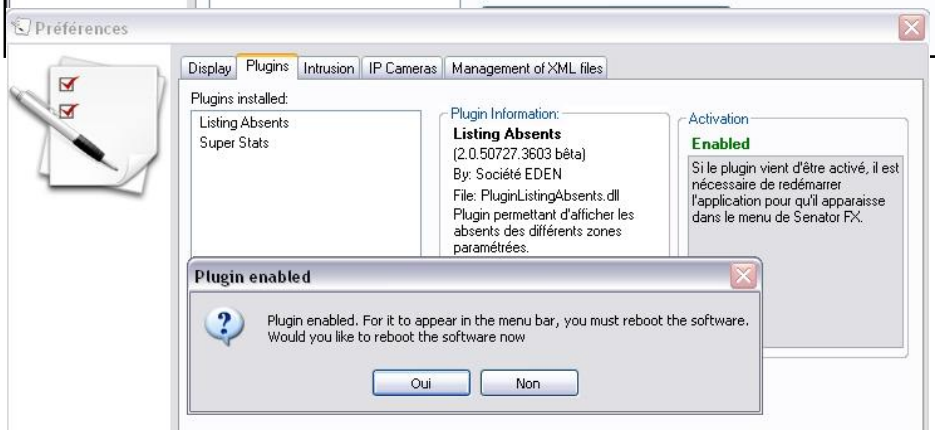
2. Cherchez votre plugin dans l'arborescence Windows, sélectionnez-le et cliquez sur "Ouvrir".

3. Une fois votre plugin ajouté, sélectionnez le dans la liste des "Plugins installés". Par défaut, le plugin est désactivé. Pour l'activer, prenez contact avec nos services qui vous fourniront une clé d'activation en fonction de votre code d'activation.

4. Une fois votre plugin activé, vous devez redémarrer votre session pour que celui apparaisse dans le menu de SenatorFX.NET.







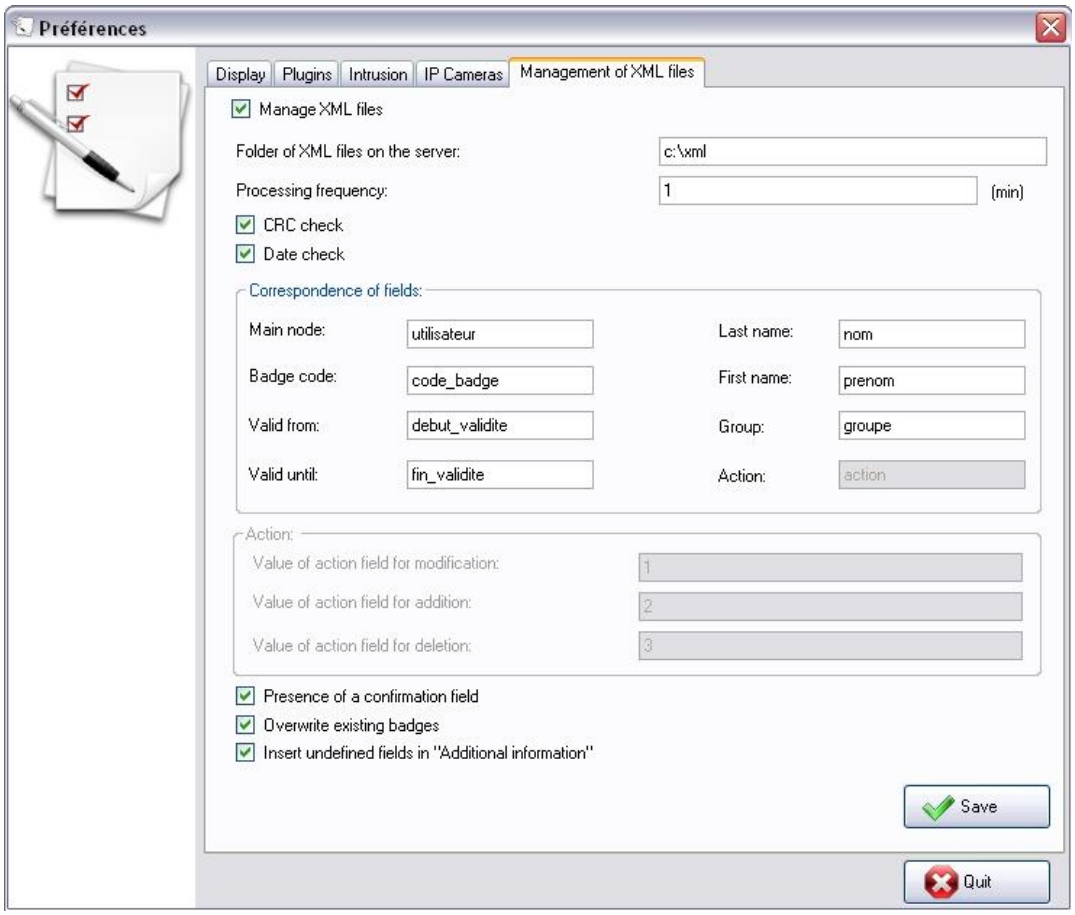
Les extensions « logiciel »

Gestion des fichiers XML

Sélectionnez extensions → Préférences

Cette application permet l'importation automatique d'une base de données tierce sous le format XML

Sélectionnez l'onglet
« Gestion des fichiers XML »



Ce formulaire va vous permettre de réaliser le « mapping » entre votre fichier XML et SenatorFX.net

« Dossier des fichiers XML »
Dossier local contenant les fichiers XML. Les fichiers XML présents dans ce dossier seront traités un par un, du plus ancien au plus récent.

« Fréquence de traitement »
Temps en minutes entre deux traitements des fichiers XML.

« Contrôle du CRC »
indique si un champ <crc></crc> est présent dans votre fichier XML et si celui-ci doit être contrôlé. Ce champ CRC permet de vérifier la validité d'un fichier XML et est calculé selon un algorithme particulier appliqué au contenu du fichier XML. Pour de plus amples informations concernant la méthode de calcul, merci de bien vouloir prendre contact avec nos services.

« Contrôle de la date »
indique si un champ <date_fichier> </date_fichier> est présent dans votre fichier XML et si celui-ci doit être contrôlé. Si cette option est coché, le fichier XML en cours de traitement devra obligatoirement avoir une « date_fichier » plus récente que celle du dernier fichier traité.

Les extensions « logiciel »

Gestion des fichiers XML

Description détaillée de l'importation d'une base de données au format XML.

Nœud principal
il ne s'agit pas du nœud principal de votre fichier XML mais du nœud englobant toutes les informations du badge.
Ce champ doit être obligatoirement renseigné et contenir le nom du nœud.

« Code badge » *
Nom du champ contenant le code du badge.
« Début de validité » *
Nom du champ contenant la date de début de validité.
« Fin de validité » *
Nom du champ contenant la date de fin de validité.
« Nom » *
Nom du champ contenant le nom d'utilisateur.
« Prénom » *
Nom du champ contenant le prénom d'utilisateur.
« Groupe » *
Nom du champ contenant le groupe d'utilisateur, tel qu'il est défini et orthographié sous SenatorFX.

***Si vous ne souhaitez pas éditer d'information, ces champ devront être créés et pourront contenir une valeur nulle.**
« Action »
Nom du champ contenant l'action à effectuer pour un badge donné. Champ obligatoire si « Présence d'un champ de validation » est décoché. Dans le cas contraire, « action » ne sera pas pris en compte.
Action :
- Valeur champ action pour modification : valeur que prendra le champ « action » pour effectuer une modification sur un badge.
- Valeur champ action pour ajout : valeur que prendra le champ « action » pour effectuer un ajout de badge.
Valeur champ action pour suppression : valeur que prendra le champ « action » pour effectuer une suppression de badge.

« Présence d'un champ de validation »
Indique si votre fichier contiendra par badge un champ <Validé /> ou <Annulé />, permettant respectivement d'ajouter ou de supprimer un badge.

« Écraser les badges déjà existant »
Indique si le fait d'ajouter un numéro de badge déjà existant dans SenatorFX écrasera le précédent. Si cette case n'est pas cochée, l'action d'ajout sera annulée si le code badge existe déjà.

« Insérer les champs non définis dans « Informations complémentaires »
Indique si les champs contenus dans votre fichier XML et non définis précédemment doivent être insérés dans les informations complémentaires de la fiche du badge. Nous verrons plus loin qu'il est préférable de ne pas cocher cette case et d'ajouter un nœud <info_complémentaires> à votre fichier XML.

Il est à noter que les valeurs entrées pour les champs « Nœud principal », « Code badge », « Début de validité », « Fin de validité », « Nom », « Prénom », « Groupe » et « Action » doivent respecter la norme XML et, de ce fait, ne pas contenir d'accents, d'espaces ou autres caractères spéciaux.

Le suivi des ajouts, modifications et suppressions de badges par traitement de fichiers XML est disponible dans l'onglet « administration », option « journal de bord ».

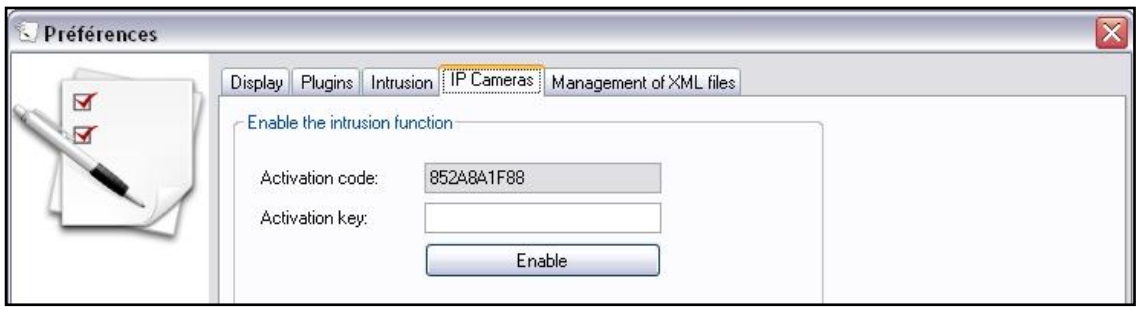
Les extensions « logiciel »

Activation de la gestion des caméras IP

Sélectionnez extensions → Préférences

La fonction « Caméras IP" permet de piloter les caméras IP Axis avec SenatorFX.NET. (cette application est décrite page 119)

Sélectionnez l'onglet « Caméras IP »



Cette fonction n'est pas activée par défaut. Pour l'activer, prenez contact avec nos services qui vous fourniront une clé d'activation en fonction de votre code d'activation.

Préférences
Display
Plugins
Intrusion
IP Cameras
Management of XML files
Enable IP Camera function
Si la fonction intrusion vient d'être activée, il est nécessaire de redémarrer l'application pour qu'elle apparaisse dans le menu de Senator FX.
Function enabled

Une fois la fonction Caméras IP activée, vous devez redémarrer votre session pour qu'elle apparaisse dans le menu de SenatorFX.NET.

Les extensions « logiciel »

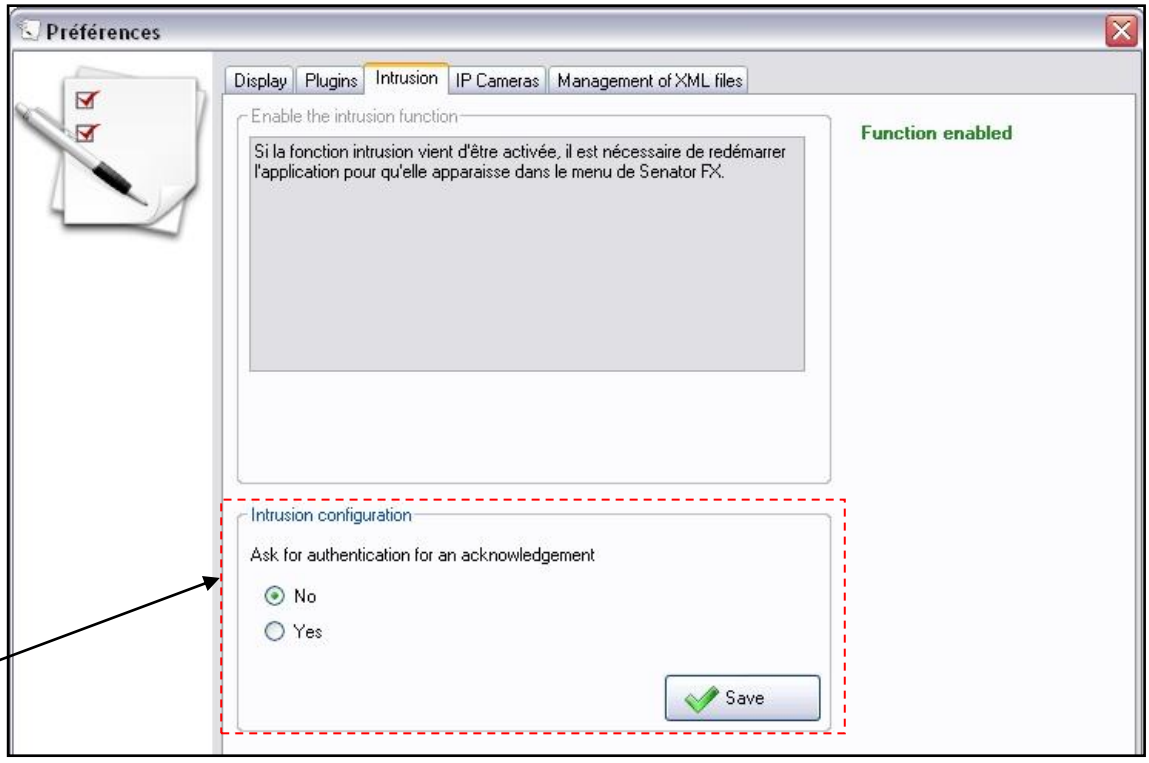
Activation de la gestion des centrales d'alarme GALAXY

Sélectionnez extensions → Préférences

La fonction « Intrusion » permet de piloter les centrales d'alarme Intrusion GALAXY « Dimension » avec SenatorFX.NET. (voir description page111).

Choisissez l'onglet Intrusion

Cette fonction n'est pas activée par défaut. Pour l'activer, prenez contact avec nos services qui vous fourniront une clé d'activation en fonction de votre code d'activation.



Paramétrage Intrusion

Permet de demander une authentification pour un acquittement d'alarme intrusion.

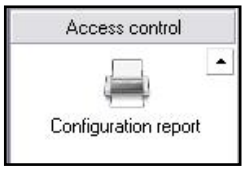
Une fois la fonction Intrusion activée, vous devez redémarrer votre session pour qu'elle apparaisse dans le menu de SenatorFX.NET.

Les extensions « logiciel »

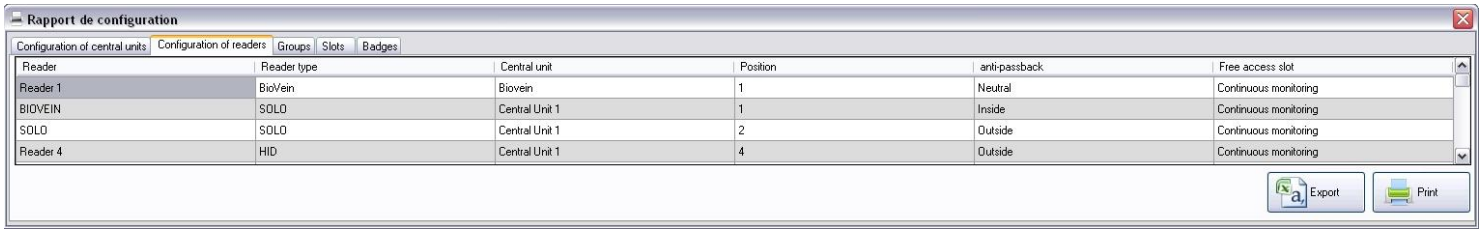
Rapport de configuration

Sélectionnez Contrôle d'accès → Rapport de configuration

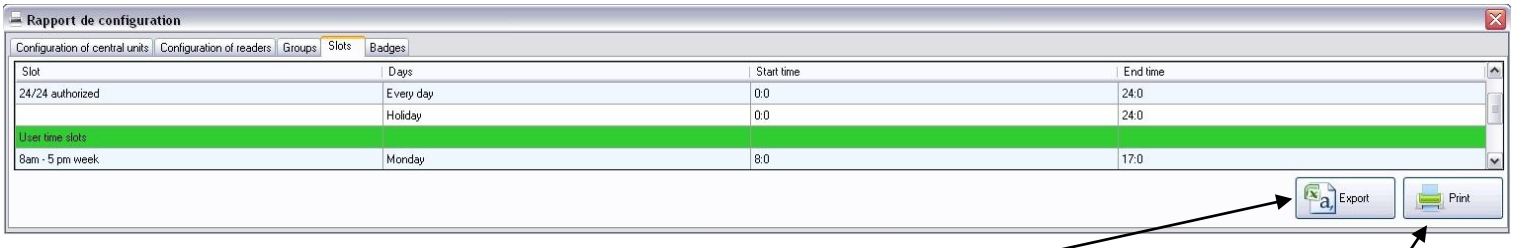
Cette option permet d'imprimer le paramétrage complet du site.



Cliquez sur « Rapport de configuration »



Onglet	Description
Configuration des centrales	Libellé de la centrale, type, Adresse Bus, Profil APB, Délai Anti-timeback, délai de transit, Entrée radio, Changement d'heure, Hors connexion, Version et N° de série des centrales
Configuration des lecteurs	Libellé du lecteur, type, centrale associée, position/centrale, profil APB, Plage accès libre
Groupes	Libellé du groupe, lecteurs associés, plages horaires d'accès, Groupe de sortie relais associé (gestion ascenseur), Maximum autorisé par groupe.
Plages	Libellé de la plage, droits d'accès/jour, heures début/fin des droits d'accès
Badges	N° du badge, Nom/Prénom de l'utilisateur associé, Groupe d'accès affecté, statut, locataire associé, code PIN, Crédit de passage, N° plaque d'immatriculation



Bouton « Exporter »

Exporte les données de **l'onglet actif** dans un fichier externe au format tableur.

Bouton « Imprimer »

Imprime les données de **l'onglet actif.**

Chapitre 8

Les applications « logiciel »

Que contient ce chapitre ?

Les applications « logiciel » 104
Configurer la sauvegarde automatique 106
Le temps de présence 107
Occupation des zones 108
Localiser un badge 109
Remise en cycle des badges 110
Pilotage des lecteurs 111
L'alarme Intrusion 112
1.Paramétrage des centrales 112
2.Ajouter des centrales d'alarme GALAXY 113
3.Modifier une centrale d'alarme GALAXY 114
4.Lancer la communication 115
5.Tracer le dialogue 115
6.Supprimer une centrale 115
7.Le simulateur 116
8.Afficher une centrale d'alarme GALAXY 117
9.Historique des alarmes 118
Levée de doute « Vidéo IP » 119
1.Ajouter une caméra 119
2.Modifier une caméra 119
3.Supprimer une caméra 119
4.Gestion des prépositions des dômes 120
5.Gestion des vues 121
6.Gestion des cycles 122
7.Enregistrements des photos/séquences vidéo 123
8.Rechercher les photos 124
9.Rechercher les séquences vidéo 125
Levée de doute « Vidéo via VDR» 126
1.Ajouter un DVR 126
2.Ajouter une caméra 126
3.Afficher les caméras 127
Gestion graphique du site 128
1.Ajouter un plan 128

2.Les composants 129
3.Ajouter les composants 130
4.Personnaliser les composants 131
5.La supervision 132
Liste des événements 133
1.Paramétrage des événements 133
2.Journal fil de l’eau 134
3.Les listes 135
Historique avancé 136

Les applications « logiciel »

Configurer la sauvegarde automatique

Sélectionnez l'onglet « extensions » → Configurer la sauvegarde automatique

Ce menu permet de paramétrer la fréquence de rappel de la sauvegarde de la base de données du site.

Cliquez sur « Configurer la sauvegarde automatique »

Cochez la case « activez la sauvegarde automatique »
Le menu déroulant « choisir la fréquence de rappel » vous permet de choisir la fréquence de l'enregistrement.

Il est possible de d'effectuer la sauvegarde tous les jours, toutes les semaines ou tous les mois.
Il est possible également de choisir le répertoire de destination de la sauvegarde.

Attention lorsque vous récupérez une sauvegarde, tous les événements et toutes les modifications entre la dernière sauvegarde et l'instant présent sont perdus.

Les applications « logiciels »

Le temps de présence

Sélectionnez extensions → Temps de présence

Le logiciel SENATORFX.NET est capable de calculer le temps de présence des personnes dans une zone à partir des événements d'entrée et de sortie sur le site.
Cette application ne peut en aucune manière en France être utilisée à des fins de calcul des salaires des employés.

Cliquez sur « Temps de présence »

Procédure d'utilisation

1.Sélectionnez la zone souhaitée dans le champs « Zone »
2.Sélectionnez dans le champs « sélection par » le critère d'affichage des badges/utilisateurs de la requête choisie.

- Les choix possibles sont : Nom du porteur, Numéro du badge, Groupe d'accès ou Société
- Vous pouvez réaliser un filtre sur certains badges si la sélection est « N° du badge »

3.Éditez une date et une heure de début du calcul du temps de présence
4.Éditez une date et une heure de fin du calcul du temps de présence
5.Si vous cochez la case « détailler les passages », vous obtiendrez l'affichage du détail des passages et des temps pour chaque badge dans la période et la zone indiquée.

Détails des boutons

Le bouton **« Presse papier »** (premier bouton de la barre d'outils) copie l'ensemble des éléments affichés dans le presse-papier. Ils pourront ensuite être collés dans n'importe quel tableur ou traitement de texte.
Le bouton **« Rechercher »** effectue le calcul du temps de présence.
Le bouton **« Aperçu »** (deuxième bouton de la barre d'outils) affiche un aperçu avant impression des éléments affichés.
L'impression pourra être déclenché à partir de l'aperçu.

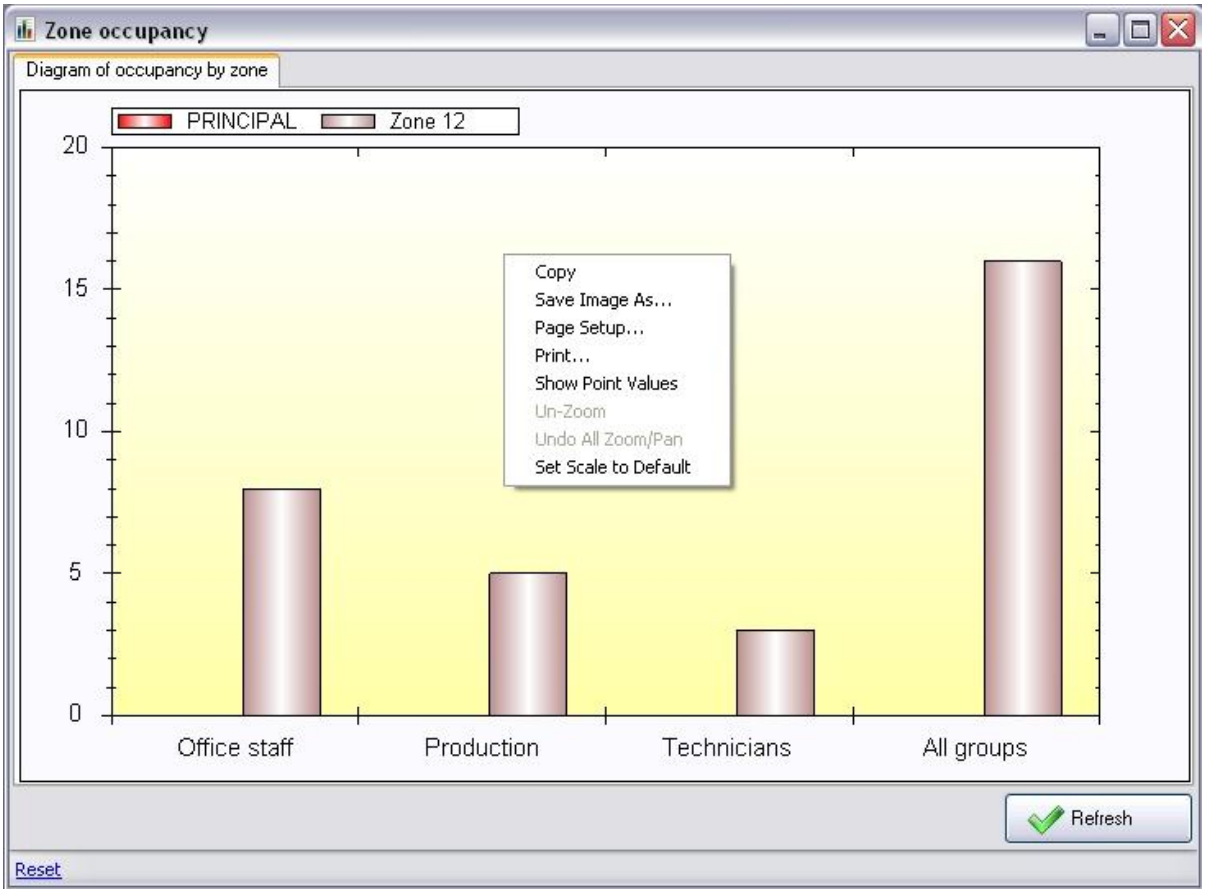
Les applications « logiciels »

Occupation des zones

Sélectionnez extensions → Occupation des zones

L'occupation des zones permet l'affichage en temps réel du nombre de personnes présentes sur le site dans chaque zone au total et par groupe d'accès.

Cliquez sur «Occupation des zones »



Un clic droit sur le graphique permet :

-Copier l'image,
-Enregistrer l'image sous…,
-Imprimer l'image affichée des présents
-Visualiser les valeurs
-Réinitialiser l'échelle

Les applications « logiciel »

Localiser un badge

Sélectionnez extensions → Localiser un badge

L'application « localiser un badge » permet la recherche du dernier passage d'un badge sur un lecteur du site à l'instant « T ».

Cliquez sur «Localiser un badge »

Procédure

1. **« Rechercher par »**

Permet de préciser le critère de recherche parmi les champs de la fiche badge:

N° du badge
Nom du porteur
Tous champs complémentaires existants

2. **« Entrer le texte recherché »**

Permet de préciser la valeur recherchée

« Dernier point de passage »

Affichage du dernier point de passage du badge/utilisateur connu par le système

« Afficher le badge »

Permet d'afficher la fiche du badge/utilisateur concerné et de voir ou modifier les informations du badge en détail.

Les applications « logiciel »

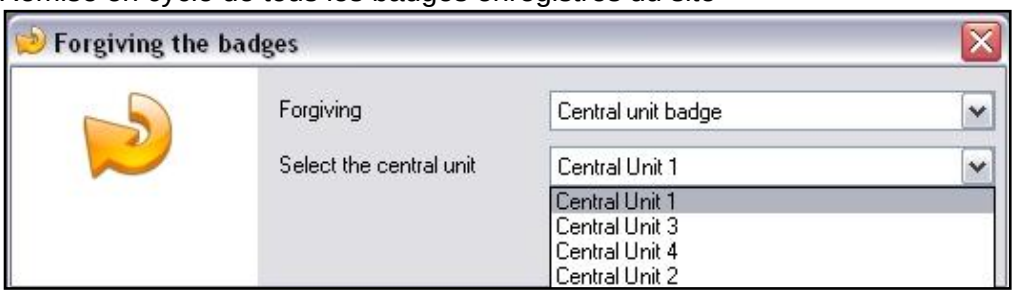
Remise en cycle des badges

Sélectionnez extensions → Remise en cycle des badges

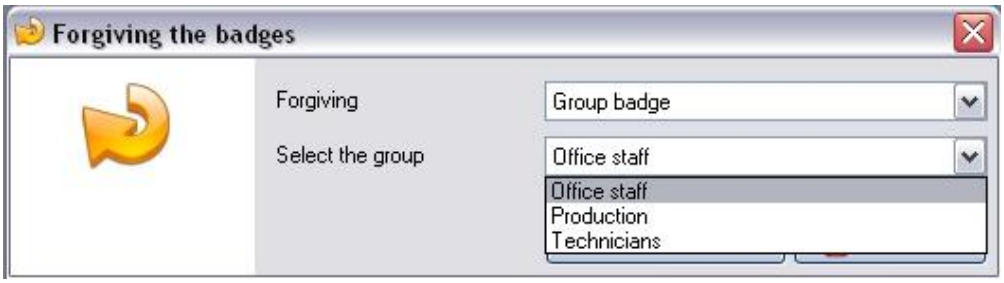
L'application « Remise en cycle des badges » effectue une RAZ (Statut « neutre ») de la position « Anti-Passback » d'un ou plusieurs badges selon l'option choisie dans le menu déroulant.

Cliquez sur « Remise en cycle des badges

« Tous les badges »
Remise en cycle de tous les badges enregistrés du site



« Badge de la centrale »
Remise en cycle de tous les badges autorisés sur la centrale sélectionnée



« Badge du groupe d'accès »
Remise en cycle de tous les badges associés au groupe d'accès sélectionné

« Badge »
Remise en cycle du badge sélectionné.

La remise en cycle des badges a pour effet de remettre les badges en « statut neutre » dans le cadre de la gestion anti-Passback du site et de vider les zones des badges concernés.

Les applications « logiciel »

Pilotage des lecteurs

Sélectionnez extensions → Pilotage des lecteurs

L'application « Pilotage des lecteurs » permet le pilotage de tous les lecteurs et des accès du site via le logiciel.

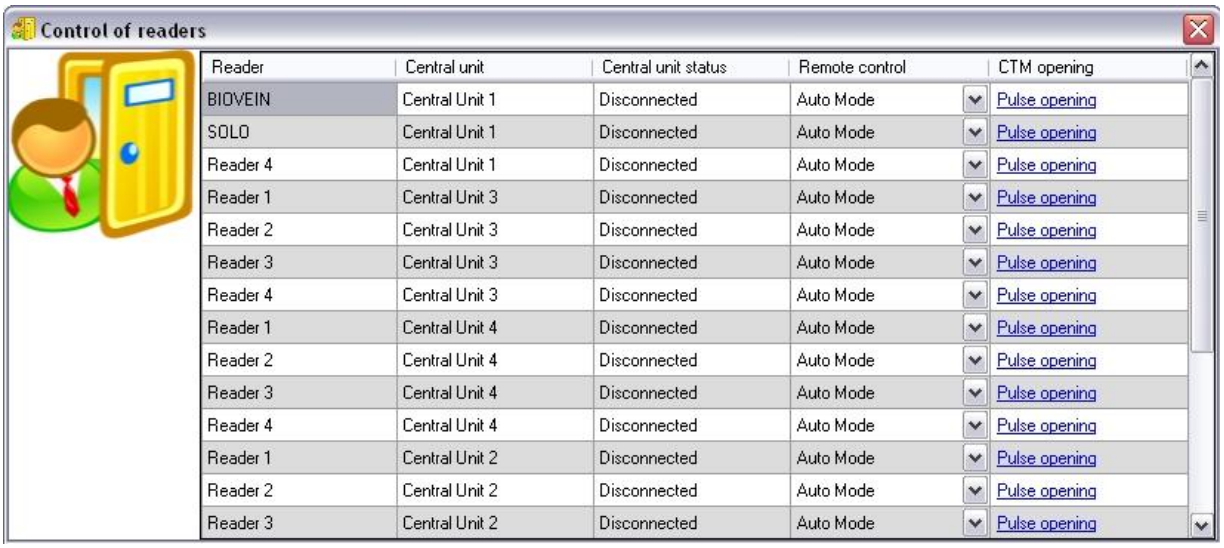
Les points à prendre en compte

- Les actions ne fonctionneront en temps réel que si la centrale sur laquelle le lecteur est connecté, dialogue avec le

logiciel, c'est-à-dire si elle est à l'état "Nominal".

- Le changement d'état du lecteur sera effectif suivant le niveau d'alerte en cours.

Cliquez sur « Pilotage des lecteurs »



Reader	Central unit	Central unit status	Remote control	CTM opening
BIOVEIN	Central Unit 1	Disconnected	Auto Mode	Pulse opening
SOLO	Central Unit 1	Disconnected	Auto Mode	Pulse opening
Reader 4	Central Unit 1	Disconnected	Auto Mode	Pulse opening
Reader 1	Central Unit 3	Disconnected	Auto Mode	Pulse opening
Reader 2	Central Unit 3	Disconnected	Auto Mode	Pulse opening
Reader 3	Central Unit 3	Disconnected	Auto Mode	Pulse opening
Reader 4	Central Unit 3	Disconnected	Auto Mode	Pulse opening
Reader 1	Central Unit 4	Disconnected	Auto Mode	Pulse opening
Reader 2	Central Unit 4	Disconnected	Auto Mode	Pulse opening
Reader 3	Central Unit 4	Disconnected	Auto Mode	Pulse opening
Reader 4	Central Unit 4	Disconnected	Auto Mode	Pulse opening
Reader 1	Central Unit 2	Disconnected	Auto Mode	Pulse opening
Reader 2	Central Unit 2	Disconnected	Auto Mode	Pulse opening
Reader 3	Central Unit 2	Disconnected	Auto Mode	Pulse opening

Définitions des colonnes de la fenêtre

« Centrale » = Toutes les centrales de gestion d'accès locales déclarées sur le site

« État centrale » = Indication de l'état de connexion en cours de la centrale. Pour que les actions soient prises en compte, l'état doit être "Nominal".

« Lecteur » = Liste des lecteurs du site que l'on va pourvoir piloter

« Télécommande » = Indication de l'état du lecteur

« Ouverture GTC » = Permet d'envoyer une commande d'ouverture à la porte contrôlée par le lecteur.

Les applications « logiciel »

L'alarme Intrusion

Sélectionnez l'onglet « Exploitation » → Intrusion GALAXY

1. Paramétrage des centrales

L'application « Alarme Intrusion » est un module optionnel du logiciel**SENATORFX.NET**.Pour la procédure d'installation et d'affichage de cette application aller à la page 102 .Elle permet d'intégrer la supervision et le pilotage des centrale d'alarme Intrusion GALAXY « Dimension ».

Les avantages

- Un seul et même logiciel pour la gestion du contrôle d'accès et des alarmes Intrusion
- Visionner l'état d'une entrée, d'une sortie ou d'un groupe en temps réel
- Piloter une entrée d'alarme d'une centrale :
  - Inclure,
  - Exclure.
- Piloter un groupe d'entrées d'alarme d'une centrale d'alarme
  - Mise en service
  - Mise en service partielle
  - Mise hors service.
- Piloter une sortie relais
  - Mode activé
  - Mode désactivé
- Toutes les informations seront supervisée via la gestion des plans dynamiques dans l'application « Supervision » et dans le monitoring « fil de l'eau ».
  Les centrales d'alarme GALAXY utilisent une liaison Ethernet.

Paramétrage de la centrale

Utilisation du clavier de la centrale pour effectuer le paramétrage.

1. Donnez le droit a l'installateur

- Composez le code Manager « 12345 » + ENT
- Allez dans le menu 48.1 et Activé le droit de l'installateur.

2. Entrez en mode installateur pour effectuer les opérations suivante

- Composez le code Manager « 112233 » + ENT

3. Configurez le module Ethernet.

- Allez dans le menu 56.4.1.1 : Indiquez l'adresse IP de la centrale
- Allez dans le menu 56.4.1.4 : Indiquez le masque de sous réseau

4. Report alarme

- Allez dans le menu 56.4.2.1 : Sélectionnez « SIA » niveau 4
- Mettez à « ON » tous les événements à gérer
- Allez dans le menu 56.4.2.2.1 : Indiquer l'adresse IP du PC qui communique avec la centrale
- Allez dans le menu 56.4.2.2.2 : Indiquer le port de communication « 10002 »
- Allez dans le menu 56.4.2.4 : Indiquer le code client « 1234 »
- Allez dans le menu 56.4.2.8 : Indiquer le protocole TCP : « 1».

5. Accès distant

- Allez dans le menu 56.4.3.1 : Sélectionnez « Toujours » pour la période d'accès
- Allez dans le menu 56.4.3.2 : Sélectionnez « Accès direct »pour le mode.

6. Commande SIA

- Allez dans le menu 56.4.8 : Indiquer l'adresse IP du pc qui communique avec la centrale.

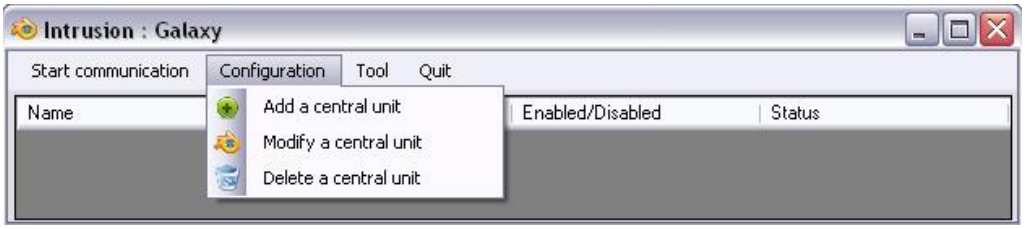
Les applications « logiciel »

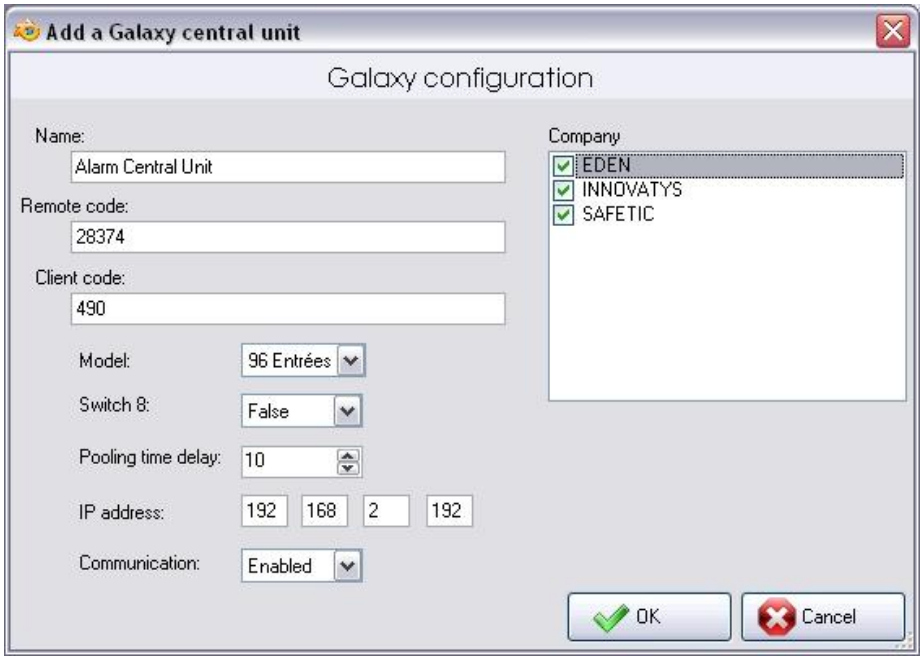
L'alarme Intrusion

Sélectionnez Exploitation → Intrusion GALAXY

2. Ajouter des centrales d'alarme GALAXY

Sélectionnez
« Paramétrage »puis « Ajouter une centrale »





Procédure

1. **Champs « Libellé »**
   Édite un nom de la centrale qui sera utilisé dans l'application et dans le logiciel
2. **Champs « Code distant »**
   Édite le code distant définit dans la centrales Galaxy (543210 par défaut)
3. **Champs « Code client »** : Édite le code client définit dans la centrale Galaxy
4. **Menu déroulant « Modèle »**
   Edite le type de Galaxy à ajouter
5. **Menu déroulant « Switch 8 »**
   Indique si le Switch 8 de la centrale est à « On » ou « Off » par défaut le switch est sur « Off »
6. **Menu déroulant « Tempo pooling »** : Configure le tempo de lectures des états.
7. **Champs « Adresse IP »**
   Édite l'adresse de la centrale sur les réseaux IP
8. **Menu déroulant « Communication »**
   Indique si la centrale doit dialoguer avec l'application ou pas.

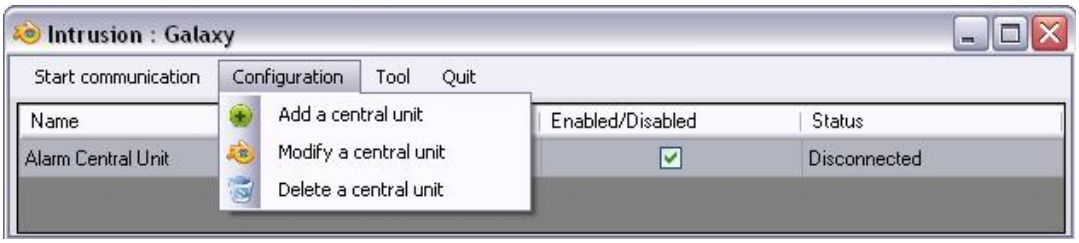
Les applications « logiciel »

L'alarme Intrusion

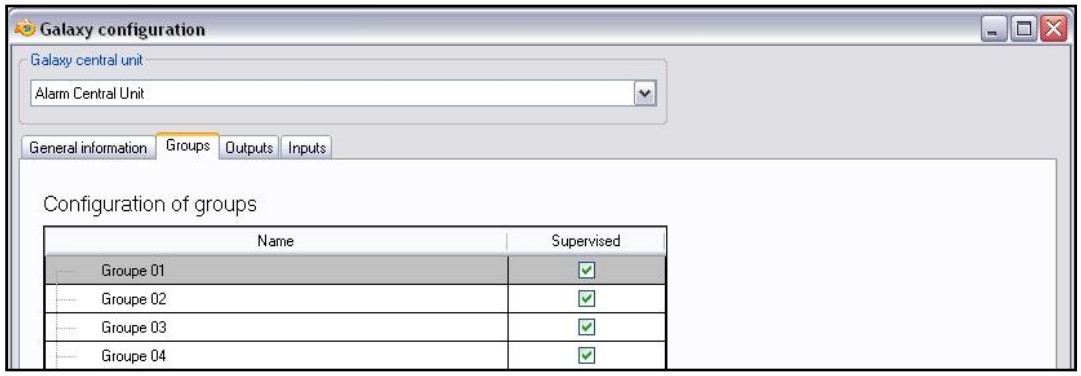
Sélectionnez l'onglet « Exploitation » → Intrusion GALAXY

3. Modifier une centrale d'alarme GALAXY

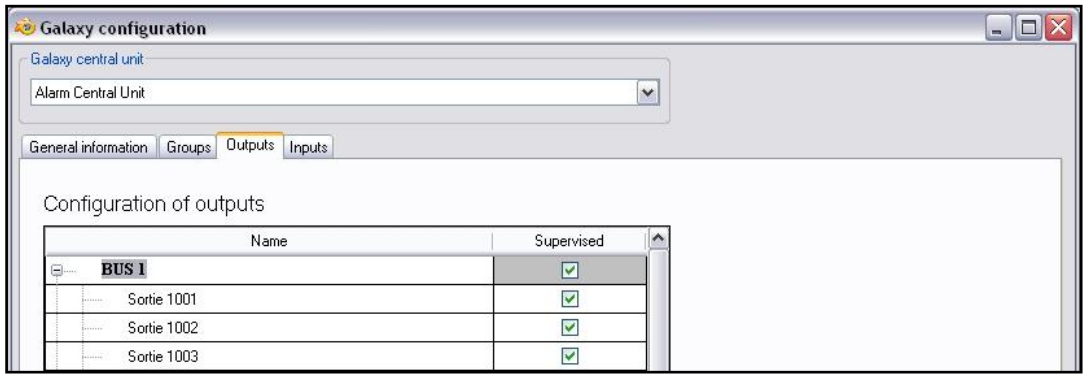
Sélectionnez « Paramétrage » puis « Modifier une centrale »



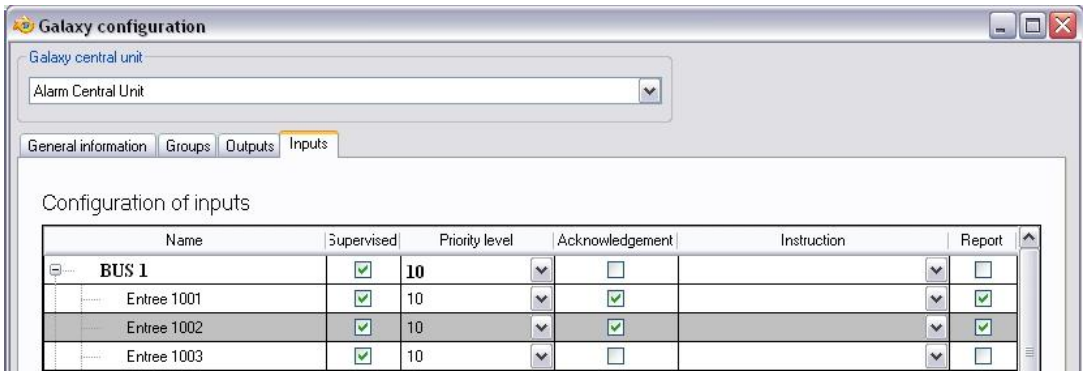
Onglet « Informations générales »
Se reporter à la page 113.



Sélectionnez la centrale souhaitée.



Onglets « Groupe, Les sorties et Les entrées »
Champ « Libellé
Éditez un libellé pour chaque entrées d'alarme, groupe ou sorties relais qui s'affichera dans le logiciel.



Case « Supervisé »
Indique si l'entrée d'alarme, groupe ou sortie relais doit être supervisé ou pas par l'application.

Case « Acquittement »
permet de définir une demande d'acquittement si l'entrée est en alarme ou en autoprotection.

Case « Consigne »
Permet de définir si une consigne doit être affichée si l'entrée est en alarme ou en autoprotection.

Case « Rapport »
Permet de définir si un rapport doit être saisi pour acquitter l'alarme ou l'autoprotection

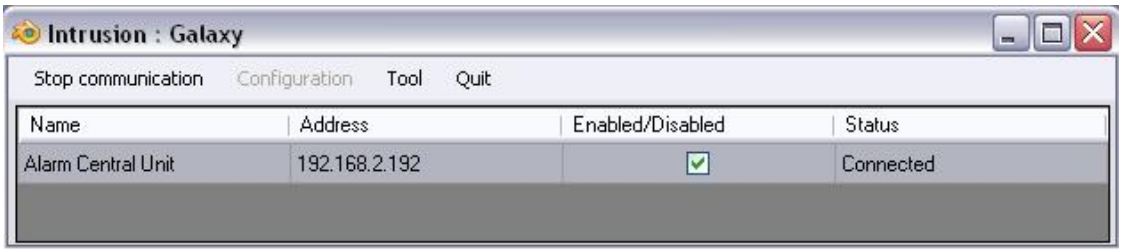
Les applications « logiciel »

L'alarme Intrusion

Sélectionnez l'onglet « Exploitation » → Intrusion GALAXY

4. Lancer la communication

Sélectionnez « Lancer la communication »



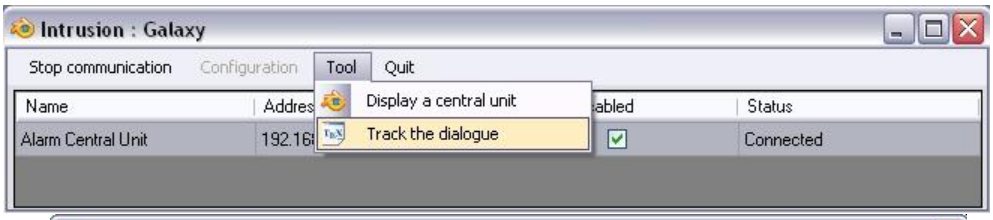
Menu « lancer la communication »
Lance la communication avec les différentes centrales de l'installation.

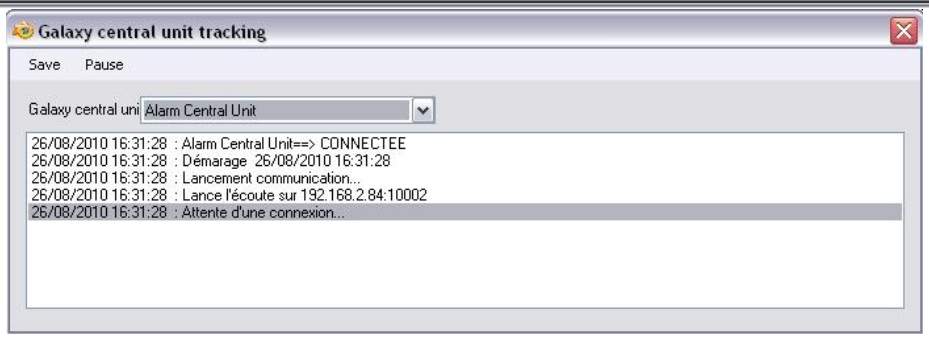
Menu « Arrêter la communication »
Arrête la communication avec les différentes centrales de l'installation.

Un message « temps réel » en bas à droite de la fenêtre principale du logiciel indique l'état de la communication.

5. Tracer le dialogue

Cliquez sur « Outil » puis « Tracer le dialogue »

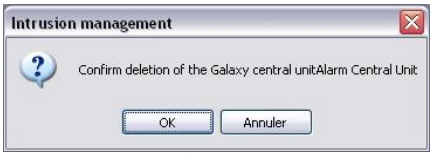


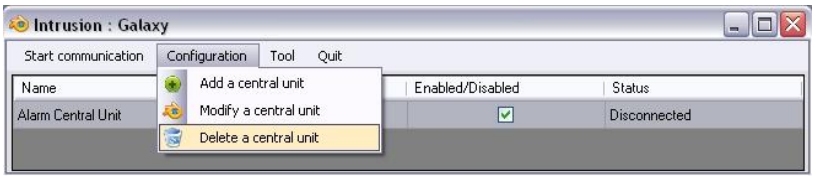

Galaxy central unit tracking
Save
Pause
Galaxy central uni
Alarm Central Unit
26/08/2010 16:31:28 : Alarm Central Unit==> CONNECTEE
26/08/2010 16:31:28 : Démarage 26/08/2010 16:31:28
26/08/2010 16:31:28 : Lancement communication...
26/08/2010 16:31:28 : Lance l'écoute sur 192.168.2.84:10002
26/08/2010 16:31:28 : Attente d'une connexion...

Ce menu permet d'afficher toutes les informations de communications entre le logiciel et les centrales d'alarme GALAXY

6. Supprimer une centrale

Sélectionner« Paramétrage »puis « Supprimer une centrale »





La suppression de la centrale d'alarme entrainera la suppression de tout le paramétrage associé

Les applications « logiciel »

L'alarme Intrusion

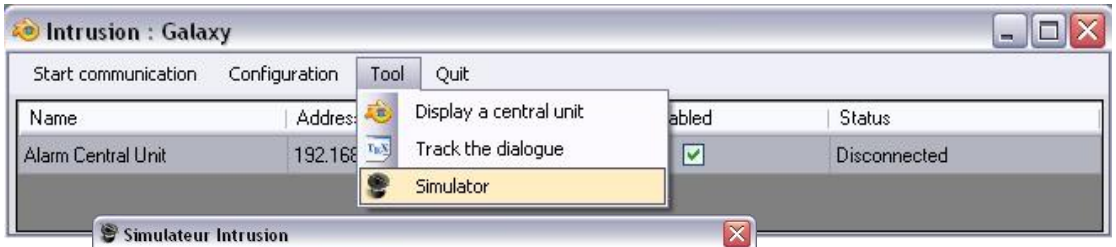
Sélectionnez l'onglet « Exploitation » → Intrusion GALAXY

7. Le simulateur

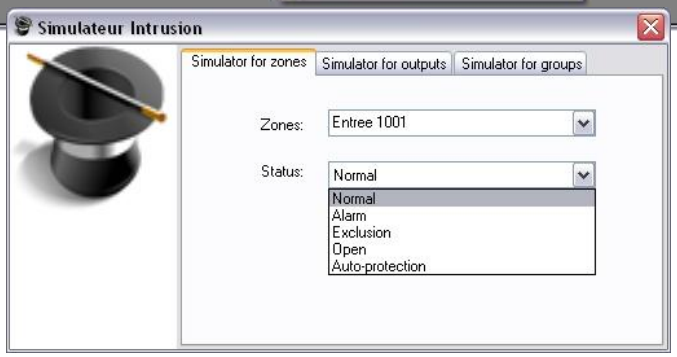
Cette fonction permet d'effectuer des démonstrations et/ou de tester les paramètres associés à une centrale d'alarme Intrusion GALAXY.

- le simulateur ne peut fonctionner que si la ou les centrales d'alarme Intrusion GALAXY ne sont pas connectées au logiciel.
- Le choix du simulateur ne s'affichera plus si une des centrales GALAXY est connectée au logiciel. Ainsi, toutes les actions déclenchées manuellement via le simulateur s'afficheront dans le journal des événements, de la supervision, etc.

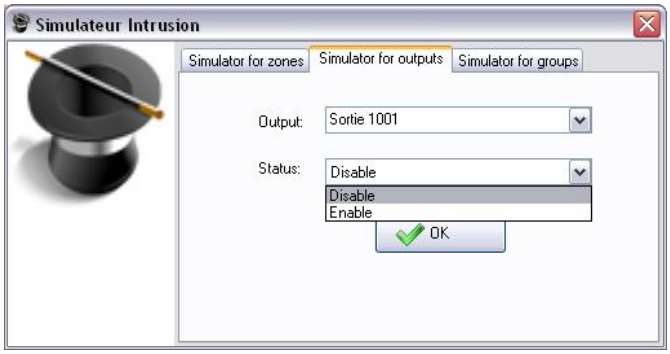
Cliquez sur « Outil »puis Simulateur



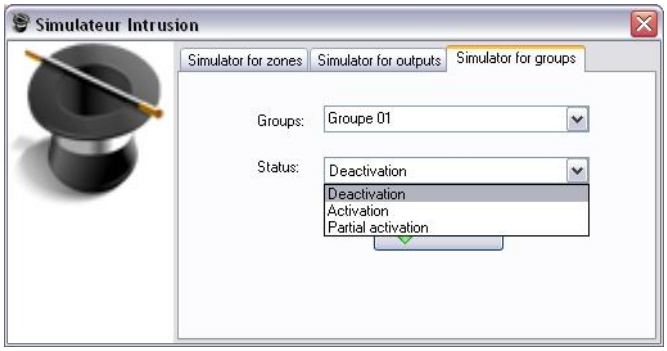
Onglet « Simulateur pour zones »
- Sélectionnez dans le menu déroulant l'entrée d'alarme souhaitée.
- Choisissez l'état et validez par le bouton « OK »



Onglet « Simulateur pour Sorties »
- Sélectionnez dans le menu déroulant la sortie relais souhaitée.
- Choisissez l'état et validez par le bouton « OK »



Onglet « Simulateur pour Groupes »
- Sélectionnez dans le menu déroulant le groupe d'entrées souhaité.
- Choisissez l'état et validez par le bouton « OK »



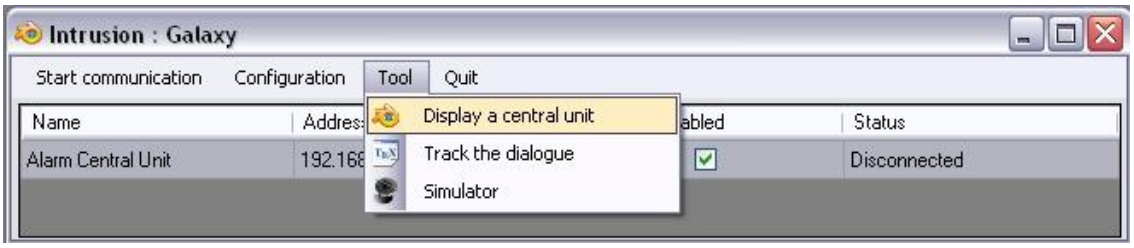
Les applications « logiciel »

L'alarme Intrusion

Sélectionnez l'onglet « Exploitation » → Intrusion GALAXY

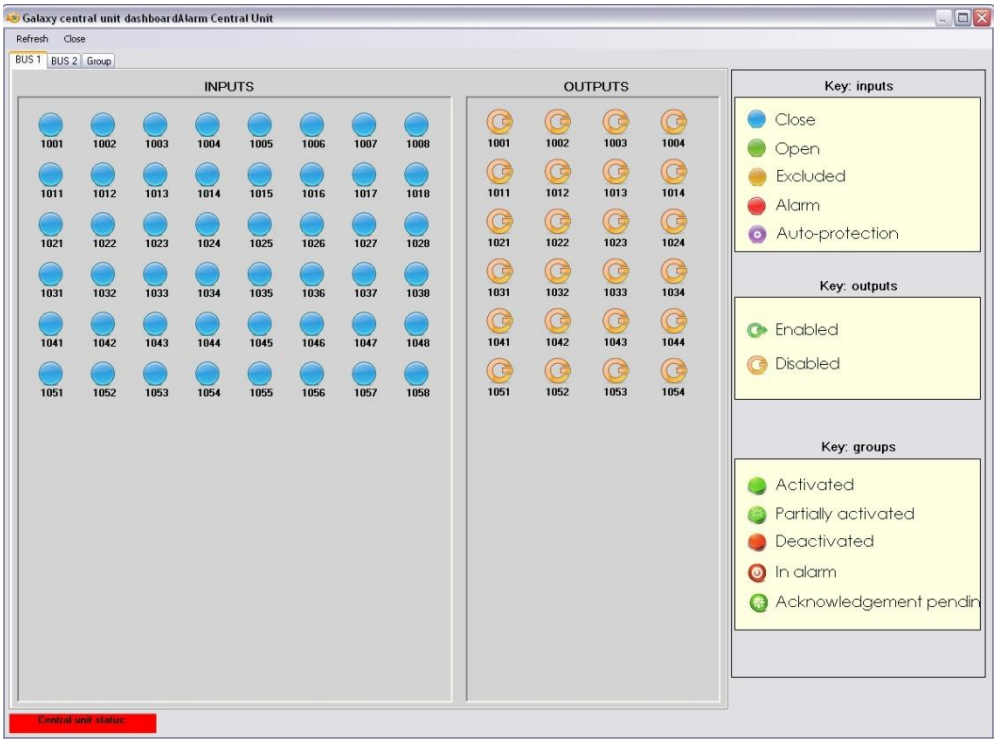
8. Afficher une centrale d'alarme GALAXY

Cliquez sur « Outil »



Sélectionnez « Afficher une centrale»

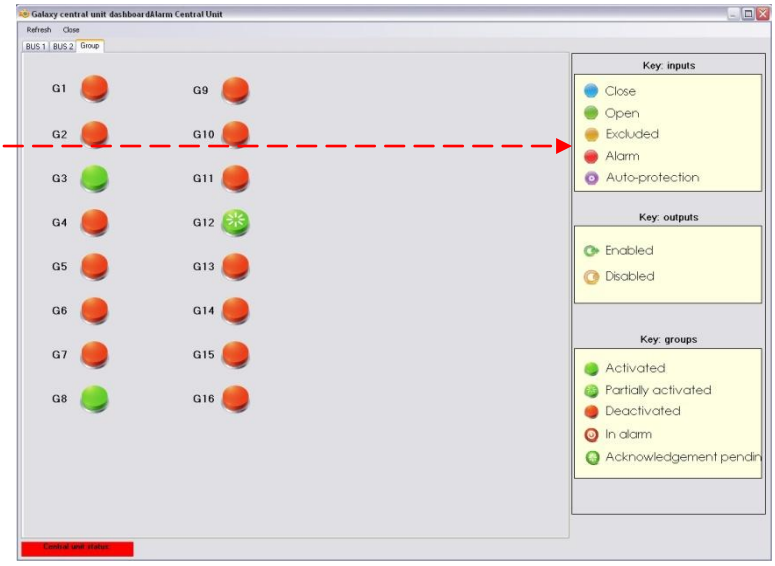
Ce menu affiche l'état en temps réel de tous les composants des centrales d'alarme GALAXY déclarées dans le logiciel. Vous pouvez sélectionner l'onglet « **BUS 1** » ou « **BUS 2** » de la centrale pour voir s'afficher l'état des entrées et sorties relais associés.



Les composants sont:

- **Entrées d'alarme**
- **Sorties relais**
- **Groupes d'entrées**

Les légendes se trouvant sur la gauche du menu affichent les états possibles des composants de la centrale d'alarme.



Les applications « logiciel »

L'alarme Intrusion

Sélectionnez l'onglet « Exploitation » → Intrusion GALAXY

9. Historique des alarmes

Ce menu permet de créer des requêtes via des filtres de recherche parmi tous les événements générés par la ou les centrales d'alarme Intrusion GALAXY gérées par le logiciel.

Cliquez sur « Historique GALAXY »

Sélectionnez une ou toutes les centrales souhaitées et vous verrez apparaître tous les événements associés à ce choix dans l'onglet « Liste des événements »

L'onglet « en attente d'acquittement » affiche les événements qui n'ont pas été acquittés.

L'onglet « Filtrer » permet d'éditer une liste d'événements suivant certains critères de recherche

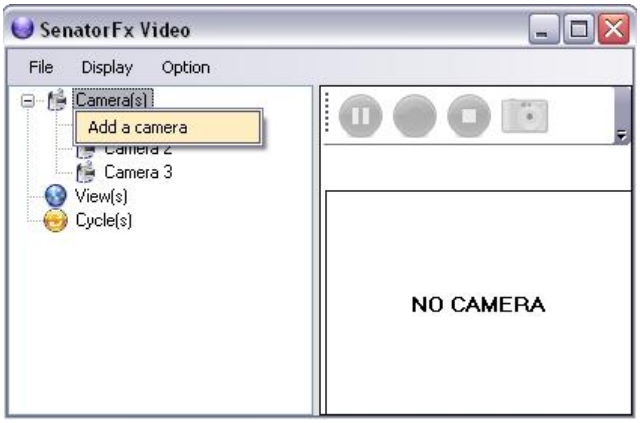
Les applications « logiciel »

Levée de doute « Vidéo IP »

Sélectionnez Exploitation → Vidéo Caméra IP

1. Ajouter une caméra

L'application « Levée de doute Vidéo IP » est un module « Plugins » optionnel du logiciel. Pour la procédure d'installation et d'affichage de cette application aller à la page 102.
Elle permet de piloter des caméras et dômes IP via le logiciel ou via des scénarios préétablis.
Cliquez sur Caméra(s)
Cliquez sur « Ajouter une caméra »

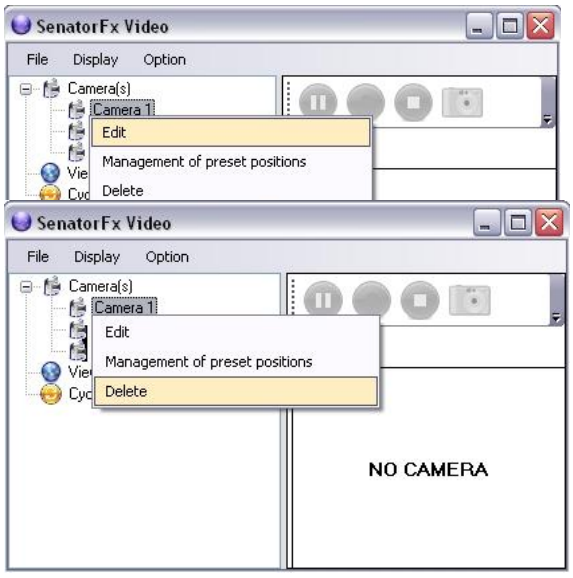


Processus

1. Éditez le libellé qui s'affichera dans le logiciel pour cette caméra
2. Éditez l'adresse IP de la caméra,
3. Éditez le « Login » pour se connecter à la caméra,
4. Éditez le Mot de passe pour se connecter à la caméra,
5. Cochez la case « Caméra mobile », s'il s'agit d'un dôme

2. Modifier une caméra

Cliquez sur « Modifier une caméra »
Effectuez les modifications souhaitées
Validez par le bouton « OK »



3. Supprimer une caméra

Cliquez sur « Supprimer une caméra »

Les applications « logiciel »

Levée de doute « Vidéo IP »

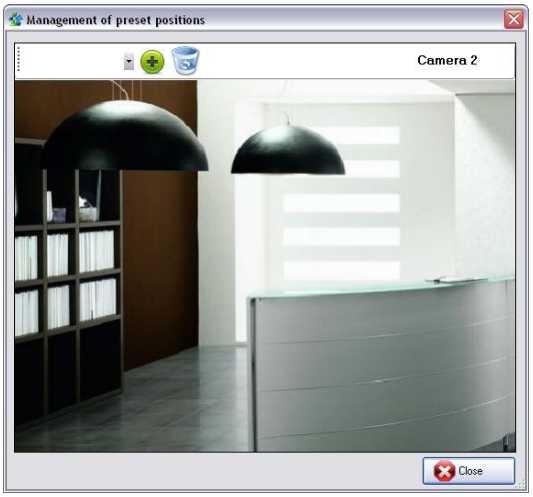
Sélectionnez Exploitation → Vidéo Caméra IP

4. Gestion des prépositions des dômes

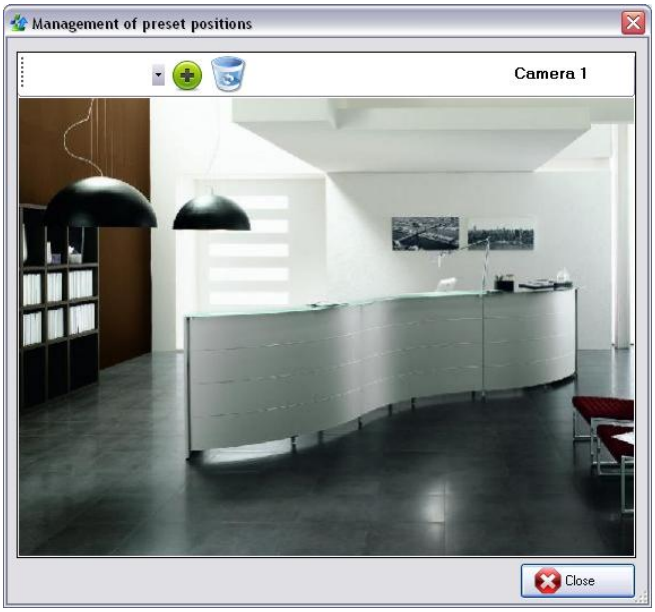
Cliquez sur Caméra(s)
Cliquez sur « Gestion des Prépositions »

Procédure

1. Utilisez les mouvements de la souris du PC afin d'éditer la position du dôme souhaitée.
2. Utilisez la molette de la souris pour fixer la position du zoom.

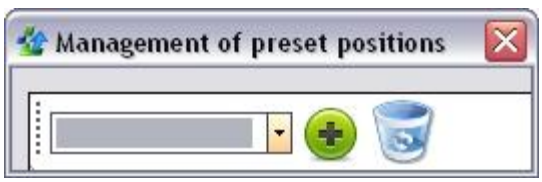


3. Cliquer sur le bouton « + » pour enregistrer le nom de la nouvelle préposition.



Pour modifiez une préposition, réitérez la même procédure.

Pour supprimer une préposition, sélectionnez là dans la liste et cliquez sur le bouton« Corbeille ».



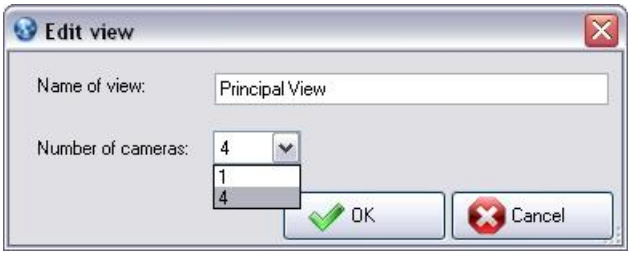
Les applications « logiciel »

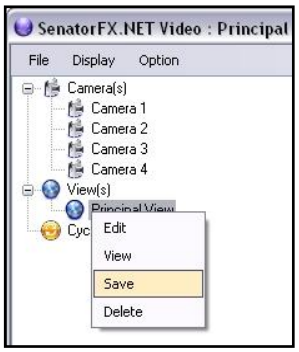
Levée de doute « Vidéo IP »

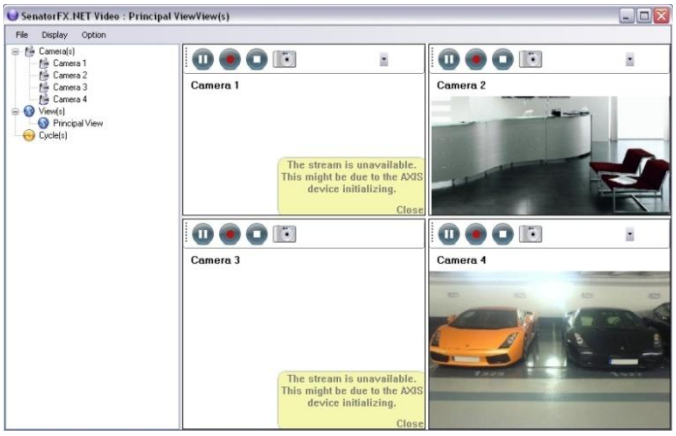
Sélectionnez Exploitation → Vidéo Caméra IP

5. Gestion des vues

Cliquez sur Vue(s)
Cliquez sur « Ajoutez une vue »







Procédure :
1.Éditez le libellé de la vue souhaitée.
2. Sélectionnez dans le menu déroulant le nombre de caméras s'affichant dans le vue.
3. Validez avec le bouton « OK ».
4**.** Placer les caméras en faisant un glisser/déplacer.
5. Une fois les caméras disposées cliquez sur la vue souhaitée et sélectionnez le menu « Enregistrer ».

Afficher une vue
Sélectionnez la vue souhaitée et cliquer sur « visualiser »

Supprimer une vue
Sélectionnez la vue souhaitée et cliquer sur « supprimer »
Puis Validez par « OK ».

Les applications « logiciel »

Levée de doute « Vidéo IP »

Sélectionnez Exploitation → Vidéo Caméra IP

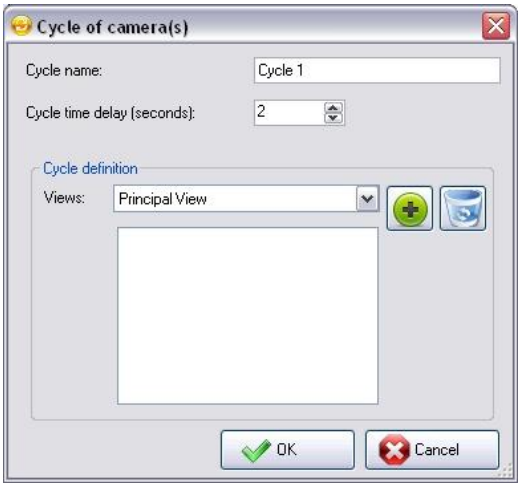
6. Gestion des cycles

Un « Cycle » est un affichage cyclique de plusieurs caméras vidéo IP selon des critères préétablis.

Cliquez sur « Ajoutez un cycle »

Procédure

1.Éditez le libellé du cycle
2. Sélectionnez le délai entre chaque vue dans le champs « Tempo cycle » (seconde)
3. Sélectionnez dans le menu déroulant « Vues » la vue souhaitée.
4. Cliquez sur le bouton « + »
5. Réitérez l'action « 4 » pour ajouter autant de vues souhaitées.
6. Pour supprimer une vue de ce cycle, veuillez sélectionner la vue à supprimer puis cliquer sur le bouton « corbeille ».
7. Validez par le bouton « OK ».



Lancer un cycle
-Sélectionnez le cycle souhaité
-Cliquez sur « Lancez le cycle »

Arrêter un cycle
Sélectionnez le cycle souhaité
Cliquez sur « Arrêter le cycle

Supprimer un cycle
Sélectionnez le cycle souhaité
Cliquez sur « Supprimer »

Les applications « logiciel »

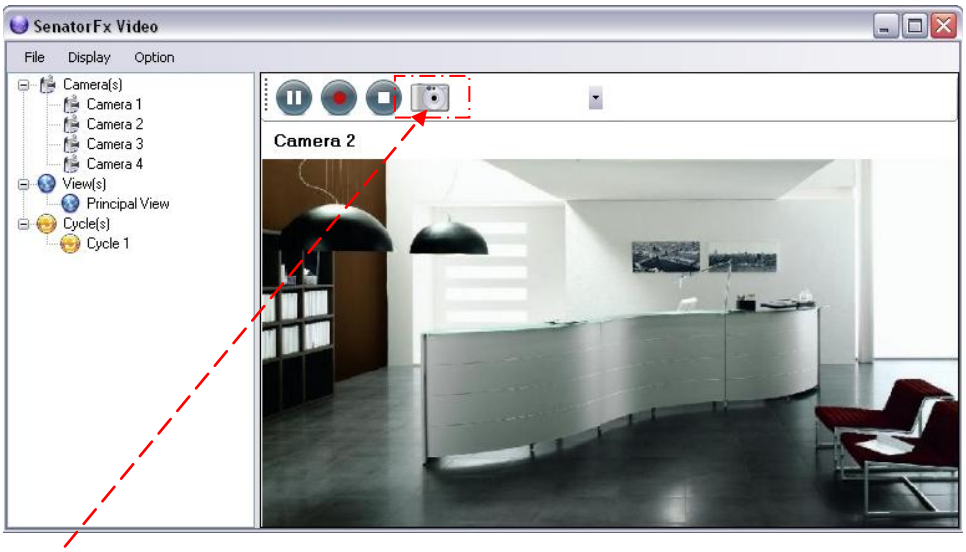
Levée de doute « Vidéo IP »

Sélectionnez Exploitation → Vidéo Caméra IP

7. Enregistrements des photos/séquences vidéo

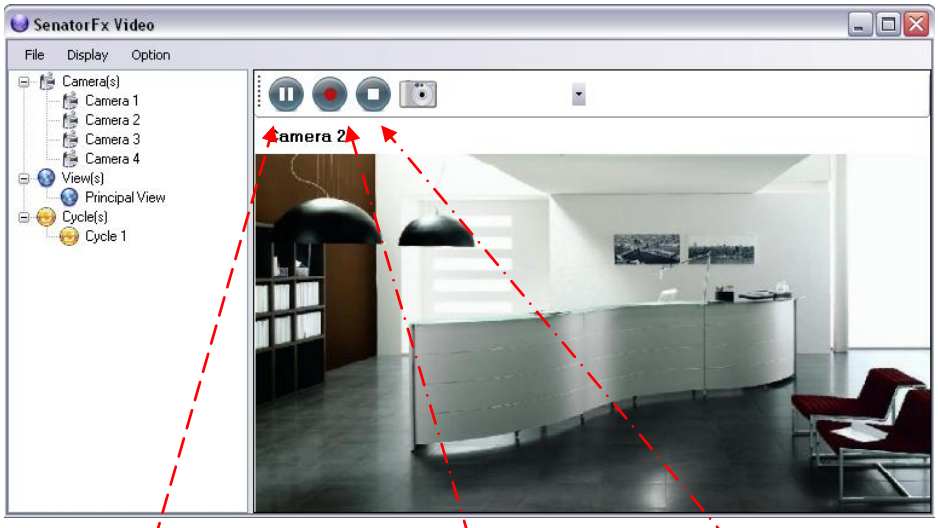
Il est possible de déclencher la prise de photo ou de séquences vidéo via le logiciel.

Cliquez sur « Vidéo IP »



Procédure d'une prise de photo :
1. Sélectionnez la caméra souhaitée,
2. Cliquez sur le bouton « appareil photo »
3.Éditez un libellé pour cette photo
4. Validez via le bouton « Enregistrer »
Les photos sont enregistrées sur la station « serveur » du logiciel

Procédure d'un enregistrement vidéo :
1. Sélectionnez la caméra souhaitée,
2. Cliquez sur le bouton « enregistrer » pour lancer l'enregistrement vidéo,
3. Cliquez sur le bouton « stop » pour stopper l'enregistrement vidéo
Les séquences vidéo sont enregistrées sur la station « serveur » du logiciel.
Un enregistrement manuel ne peut pas durer plus de 10 minutes.
Au terme des 10 minutes l'enregistrement se coupe automatiquement.



Pour effectuer une pause pendant la séquence vidéo

Pour lancer l'enregistrement manuel des séquences vidéo

Pour arrêter l'enregistrement manuel des séquences vidéo

Les applications « logiciel »

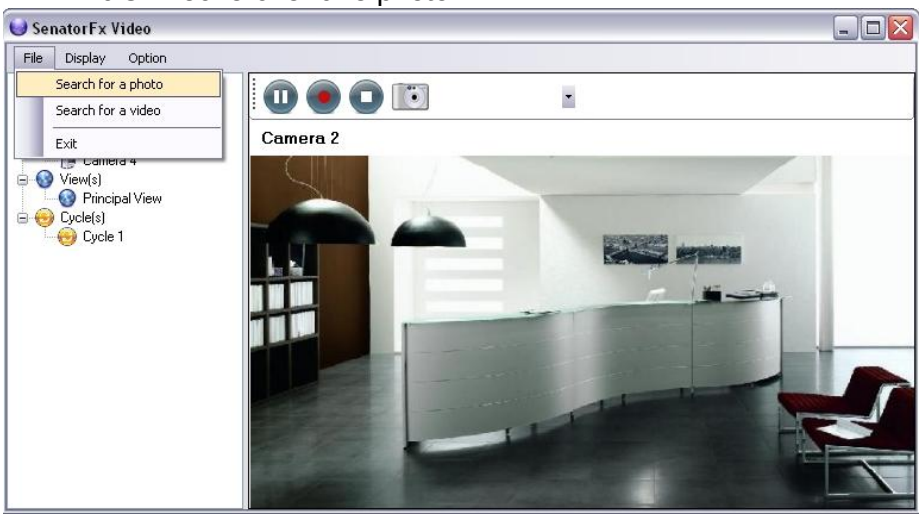
Levée de doute « Vidéo IP »

Sélectionnez Exploitation → Vidéo Caméra IP

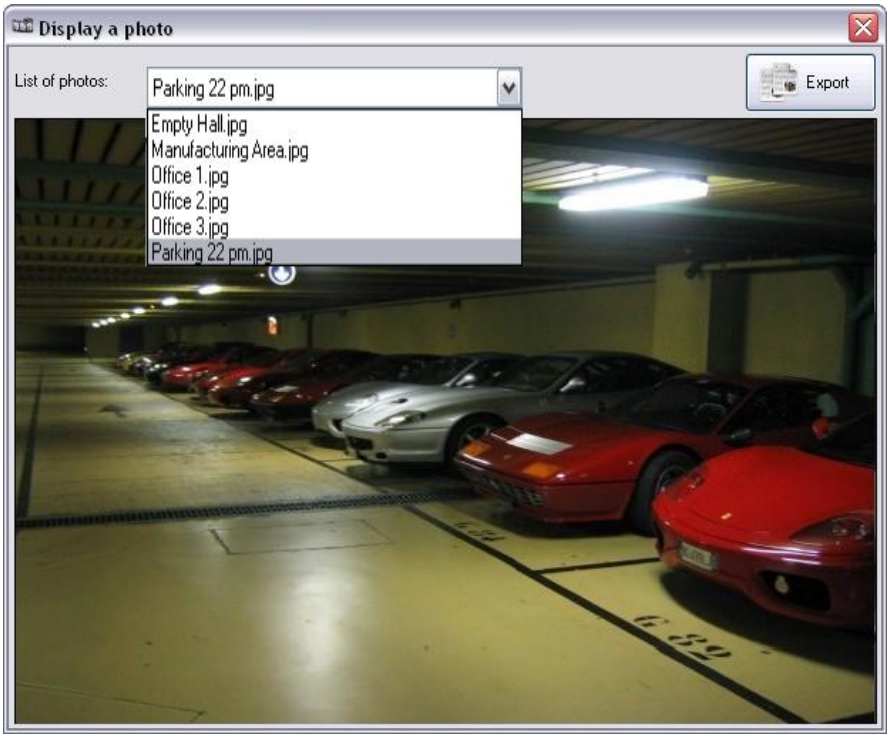
8. Rechercher les photos

Ce menu permet de rechercher et d'afficher les photos prises via les caméras et dômes vidéo IP.

- Sélectionnez « Fichier »
- Puis « rechercher une photo »



-À l'aide du menu déroulant « Liste des photos », sélectionnez la photo souhaitée,
-La photo sélectionnée s'affiche à l'écran.



Les applications « logiciel »

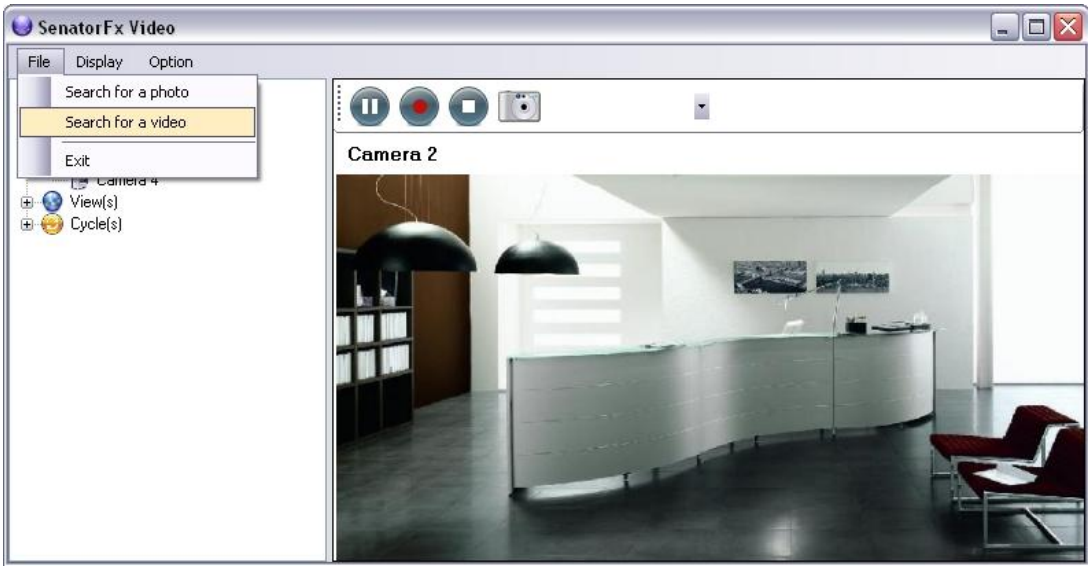
Levée de doute « Vidéo IP »

Sélectionnez Exploitation → Vidéo Caméra IP

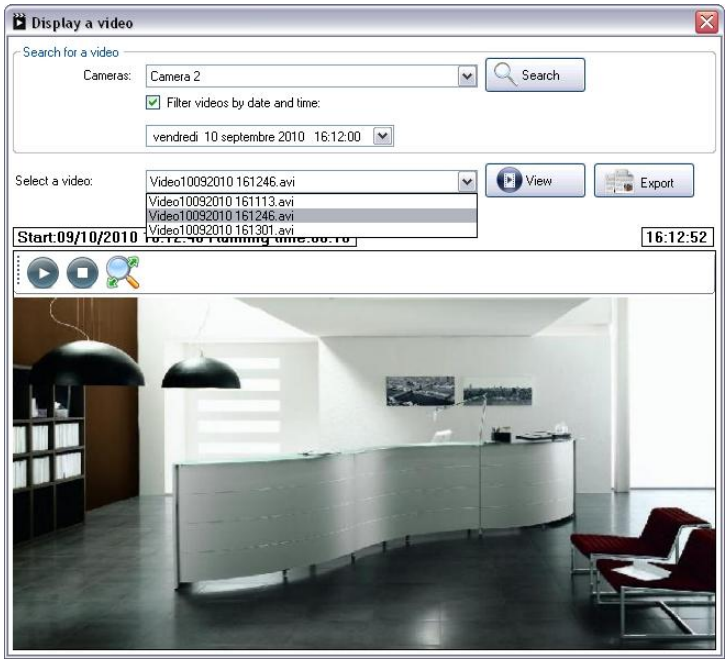
9. Rechercher les séquences vidéo

Ce menu permet de rechercher et de visualiser les séquences vidéo prises via les caméras et dômes vidéo IP.

-Sélectionnez « Fichier »
-Puis « rechercher une vidéo »



1.Sélectionnez la caméra souhaitée à partir du menu déroulant « Caméras »,
2.Cochez la case « Filtrer… » afin de sélectionner une date/heure comme filtre de recherche,
3.Cliquez sur le bouton « Rechercher »,
4.Sélectionnez la séquence vidéo souhaitée à partir du menu déroulant « Sélectionner une vidéo »,
5.Cliquez sur le bouton « Visualiser » pour lancer la séquence vidéo.



Si vous souhaitez extraire certaines séquences vidéo/photos du logiciel, veuillez vous rapprochez de la société EDEN.

Les applications « logiciel »

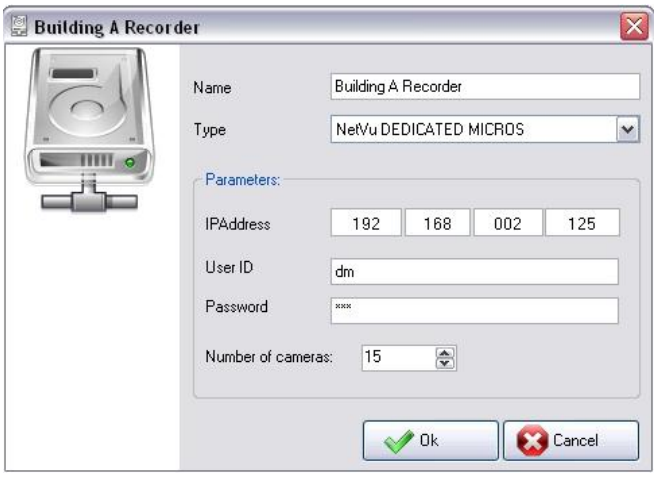
Levée de doute « Vidéo via VDR»

Sélectionnez Exploitation → Enregistreur vidéo

1. Ajouter un DVR

Cette application permet la levée de doute vidéo via des enregistreurs vidéo tiers tel le constructeur Dedicated Micros. Cela permet d'enregistrer le flux vidéo des caméras reliées sur le DVR associées à l'activité des lecteurs du site.
via des scénarios préétablis appelés « Automatismes centralisés » et suite à des événements générés par le contrôle d'accès ou par des alarmes intrusion l'on peut afficher en temps réel les caméras dans le logiciel et générer des séquences d'enregistrement vidéo qui seront stockées dans le ou les DVR

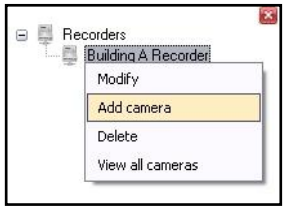
Sélectionnez « Ajouter un enregistreur vidéo ».



Procédure

1. Éditez un libellé pour l'enregistreur vidéo
2. Sélectionnez le modèle d'enregistreur dans le menu déroulant
3. Éditez l'adresse IP du DVR
4. Éditez le login et le mot de passe du DVR
5. Indiquez le nombre de caméras reliées à ce DVR

2. Ajouter une caméra



Procédure

1. Éditez un libellé pour la caméra,
2. Sélectionnez l'adresse de la caméra sur le DVR,
3. Sélectionnez le lecteur associée à cette Caméra,
4. Sélectionnez la/les sociétés associées à cette caméra.

-Cliquez sur « Enregistreur vidéo »
-Cliquez sur « Ajouter Caméra »

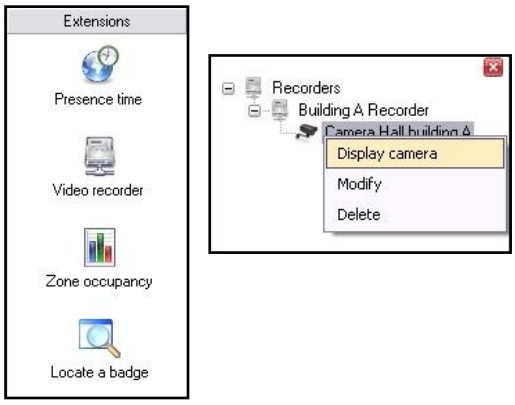
Avec cette application, le DVR enregistre en permanence le flux vidéo des caméras qui lui sont associées.
Pour les enregistrements sur événement, il faut se rapporter à la page 125

Les applications « logiciel »

Levée de doute « Vidéo via VDR»

Sélectionnez extensions → Enregistreur vidéo

3. Afficher les caméras

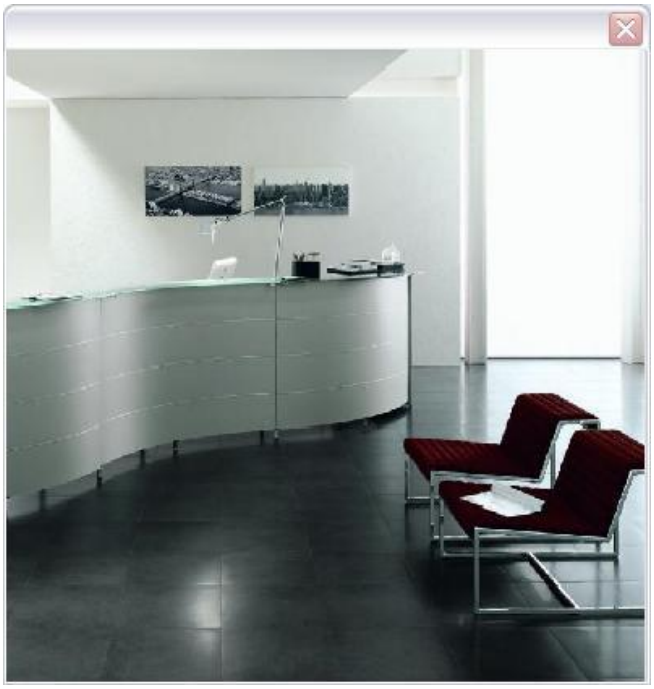


Sélectionnez un Enregistreur vidéo

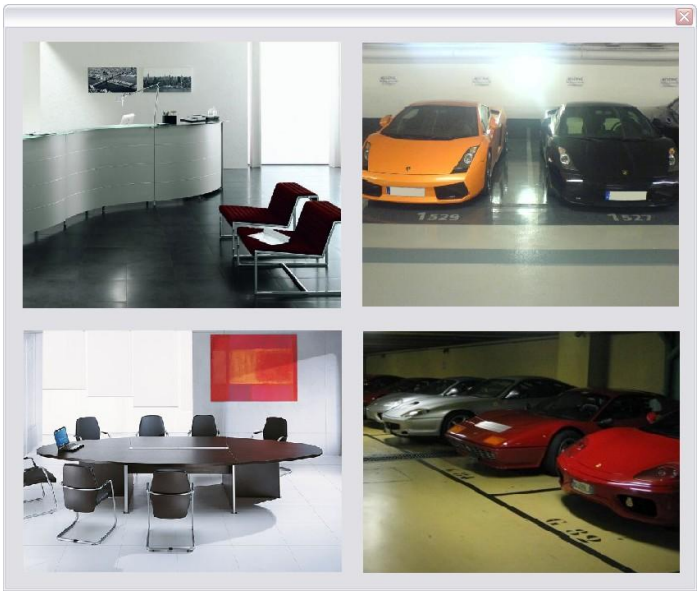
Procédure « Afficher une caméra »
1. Sélectionnez l'enregistreur puis la caméra
2. Cliquez sur « Afficher la caméra »
3. Une image vidéo « temps réelle » de la caméra sélectionnée s'affiche dans le logiciel.
4. S'il s'agit d'un dôme motorisé, vous pouvez le piloter selon les fonctions PTZ.

Il est possible de lancer l'affichage de chaque caméra à partir de l'application de supervision du site voir page 127

Pour connaitre les dômes motorisés compatibles avec le DVR, se rapporter à sa notice technique.



Procédure « Voir toutes les caméras »
1. Sélectionnez un enregistreur vidéo
2. Cliquez sur « Voir toutes les caméras ».



Les applications « logiciel »

Gestion graphique du site

Sélectionnez l'onglet « Exploitation » → Éditeur Synoptique

1. Ajouter un plan

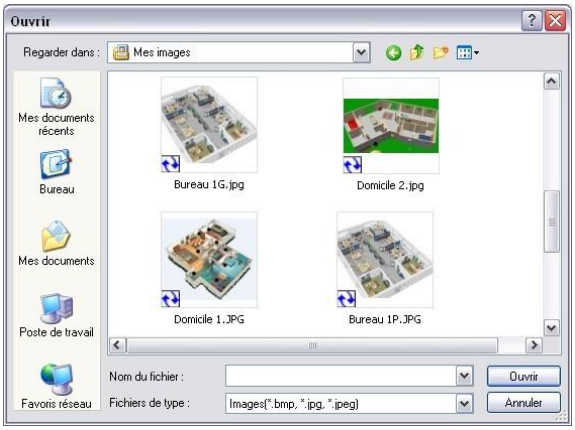
Cette application permet d'éditer le synoptique d'implantation des différents composants du site.

L'éditeur du synoptique permet le positionnement et le paramétrage des composants du site.

La gestion graphique de l'activité des accès et des alarmes du site se fait via l'application « Supervision ».

Sélectionnez Onglet « Exploitation »

Cliquez sur « Éditeur Synoptique »



Procédure « Ajoutez un plan »

1. Cliquez sous le champ « Ajouter un plan »

2. Recherchez dans la nouvelle fenêtre le répertoire ou se trouve les fichiers graphiques au format « BMP » ou « JPG »,

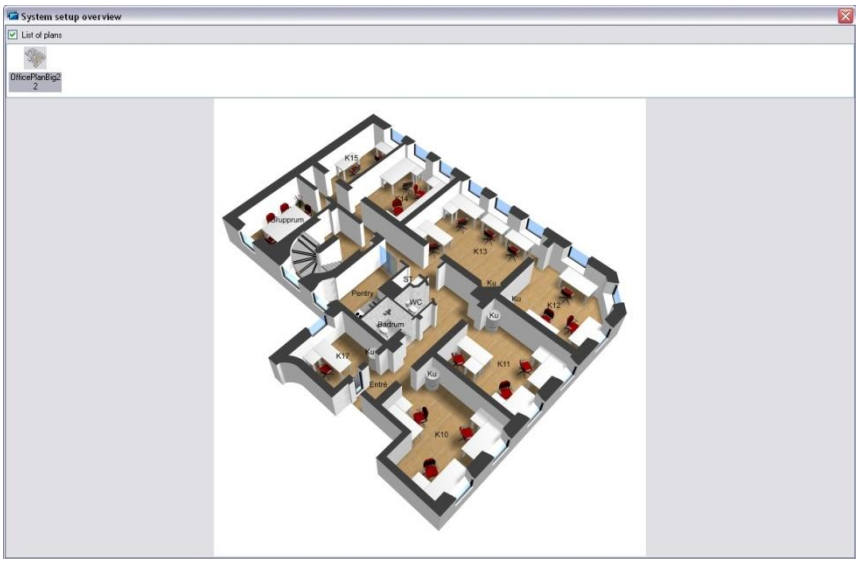
3. Sélectionnez l'image souhaitée,

4. Validez par le bouton « Ouvrir »

5. L'image du plan souhaitée apparaît et sera disponible dans les menus « Éditeur Synoptique » et « Supervision »

Réitérez cette procédure pour intégrer d'autres plans graphiques dans le logiciel. Il n'y a pas de limite de plans dans le logiciel.

Tous les plans seront visibles par tous les opérateurs du logiciel sauf les composants qui dépendent du profil du « locataire/société ».



Les applications « logiciel »

Gestion graphique du site

Sélectionnez l'onglet « Exploitation » → Éditeur Synoptique

2. Les composants

L'application « supervision » permet de connaitre l'état en temps réel des différents composants importants d'un site. Un composant peut représenter un lecteur, une centrale ou même un point d'alarme.

Composant	Description et utilité du composant dans la « Supervision »
Lecteur	Affichage de l'état de la porte contrôlée par un lecteur Affichage de la photo de l'utilisateur lors de son passage Télécommande et changement de l'état de la porte par l'opérateur
Automatisme	Affichage de l'état d'un automatisme associé à une centrale Ce type d'automatisme est géré par la centrale et ne dépend pas de l'état du logiciel
Compteur	Affichage de l'état d'un compteur associé à une centrale Changement du niveau du compteur manuellement Ce type de compteur est géré par la centrale et ne dépend pas de l'état du logiciel
Compteur global	Affichage de l'état d'un compteur associé à plusieurs centrales Changement du niveau du compteur manuellement Le compteur global est géré par le logiciel et dépend de son état
Automatisme centralisé	Affichage de l'état d'un automatisme associé à une ou plusieurs centrales Force l'exécution de l'automatisme manuellement L'automatisme centralisé est géré par le logiciel et dépend de son état
Caméra	Affiche automatiquement le flux vidéo d'un caméra IP via un automatisme Pilote les fonctions PTZ et le zoom d'un dôme Affiche le flux vidéo manuellement avec prise de photo et enregistrement vidéo
Plan	Lien/raccourci pour circuler de plan en plan
Caméra analogique	Affiche automatiquement le flux vidéo d'une caméra associée à un DVR via un automatisme Pilote les fonctions PTZ et le zoom d'un dôme Affiche le flux vidéo manuellement
Niveau d'alerte	Affiche le niveau d'alerte pour la gestion de crise Modifie manuellement le niveau d'alerte en cours
Groupe GALAXY	Affiche l'état d'un groupe d'entrées d'alarme Intrusion d'une centrale GALAXY Modifie l'état d'un groupe manuellement
Entrée GALAXY	Affiche l'état d'une entrée d'alarme Intrusion d'une centrale GALAXY Modifie l'état d'une entrée d'alarme manuellement
Sortie GALAXY	Affiche l'état d'une sortie relais d'une centrale GALAXY Modifie l'état d'une sortie relais manuellement

Les applications « logiciel »

Gestion graphique du site

Sélectionnez l'onglet « Exploitation » → Éditeur Synoptique

3. Ajouter les composants

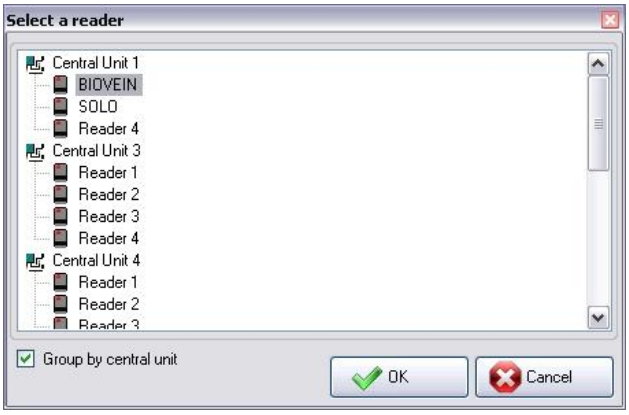
Sélectionnez un plan
Puis clic « droit » sur le plan

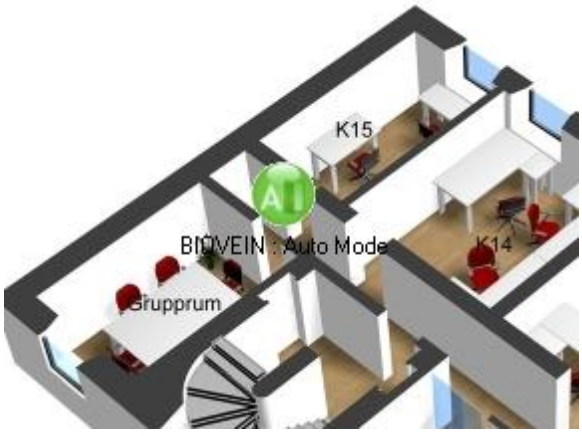
Quels composants du site ajouter?
Un lecteur qui contrôle une porte
Un Automatisme associé à une centrale
Un compteur associé à une centrale
Un compteur global géré par le logiciel
Un automatisme centralisé géré par le logiciel
Une caméra IP géré par le module optionnel
Un lien d'un autre plan graphique
Une caméra reliée à un DVR
Un niveau d'alerte pour la gestion de crise
Un groupe d'entrées d'alarme Intrusion
Une entrée d'alarme Intrusion
Une sortie relais de centrale d'alarme Intrusion

Tous les composants sont représentés par des icônes personnalisables.
Il est possible d'importer des icônes tiers au format « ICO » dans le logiciel.

Procédure « Ajouter un composant »

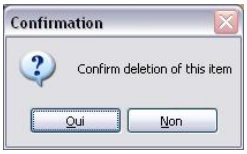
1. Pour ajouter un élément sur un plan, sélectionnez ce plan dans la liste des plans
2. À l'endroit ou vous souhaitez ajouter un composant du site effectuez un clic/droit avec la souris du PC,
3. Sélectionnez le composant souhaité (exemple un lecteur)
4. Sélectionnez le lecteur souhaité et validé par le bouton « OK »
5. Un nouvel icône apparaît sur le plan souhaité





Déplacement d'un composant
Pour déplacer un élément sur le plan, effectuez un clic gauche dessus, maintenez le bouton gauche enfoncé puis déplacez votre souris, puis relâchez le bouton gauche quand l'élément est à l'endroit souhaité.

Suppression d'un composant



Effectuez un clic droit avec la souris sur cet élément et choisissez l'option "Supprimer".
Validez avec le bouton « Oui »

Les applications « logiciel »

Gestion graphique du site

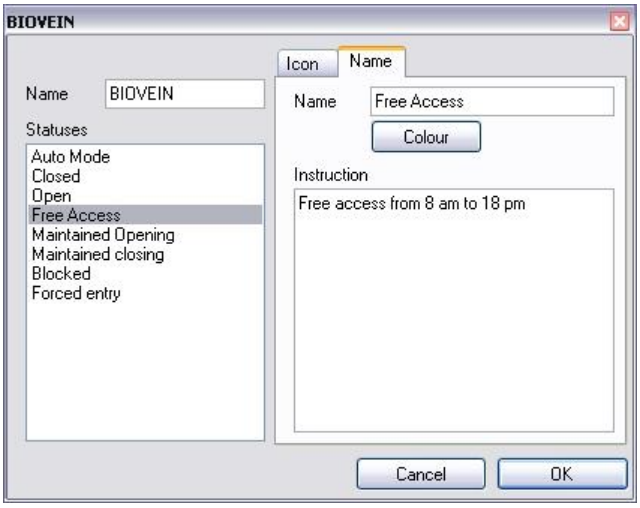
Sélectionnez l'onglet « Exploitation » → Éditeur Synoptique

4. Personnaliser les composants

Sélectionnez un plan

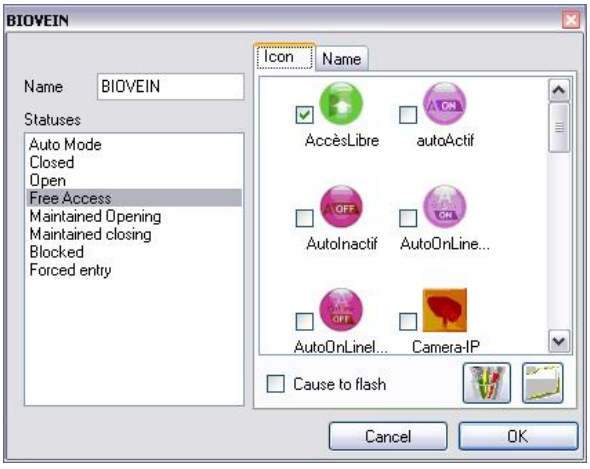
Personnalisez l'icône d'un composant

-Sélectionnez l'icône d'un composant,
-Effectuez un clic droit,
-Sélectionnez « Personnaliser »



Procédure « Onglet libellé »

- Sélectionnez un des états affichés du composant
- Sélectionnez l'onglet « Libellé »
- Modifiez le libellé de l'état du composant si besoin (le libellé est le statut de l'état du composant qui s'affiche sur la supervision en temps réel)
- Éditez la couleur du libellé si nécessaire
- Éditez une consigne si nécessaire.
- Effectuez la même procédure pour tous les états disponibles du composant.



Procédure « Onglet Icône »

- Sélectionnez un des états affichés du composant
- Sélectionnez l'onglet « Icône »
- Sélectionnez une icône disponible dans le menu déroulant
- Pour faire clignoter l'icône pendant la durée de l'état sélectionné, cochez la case « Faire clignoter »
- **Si les icônes proposés ne vous conviennent pas, vous pouvez en cliquant sur le bouton « dossier » importer un icône au format « ICO »**
- Effectuez la même procédure pour tous les états disponibles du composant.

Les applications « logiciel »

Gestion graphique du site

Sélectionnez l'onglet « Exploitation » → Supervision

5. La supervision

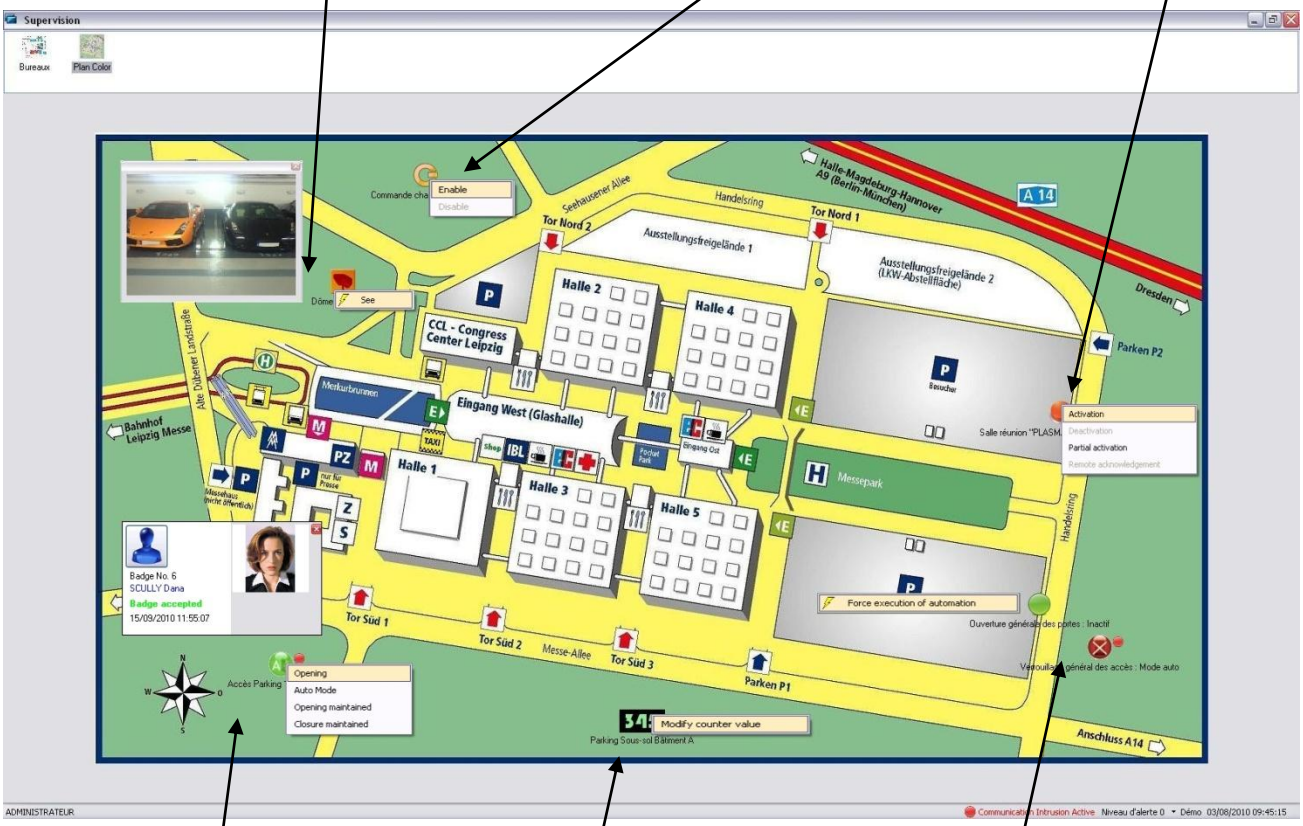
Cette application permet la localisation immédiate et graphique de l'activité des accès et des alarmes du site ainsi que de télécommander certains composants le permettant.

- Sélectionnez Onglet « Exploitation »
- Cliquez sur « Supervision »

Pilotage/affichage d'une caméra IP

Pilotage/affichage d'une sortie de centrale d'alarme

Pilotage/affichage d'une zone d'alarme



Pilotage/affichage d'un accès contrôlé

Pilotage/affichage d'un compteur

Pilotage/affichage d'un Automatisme

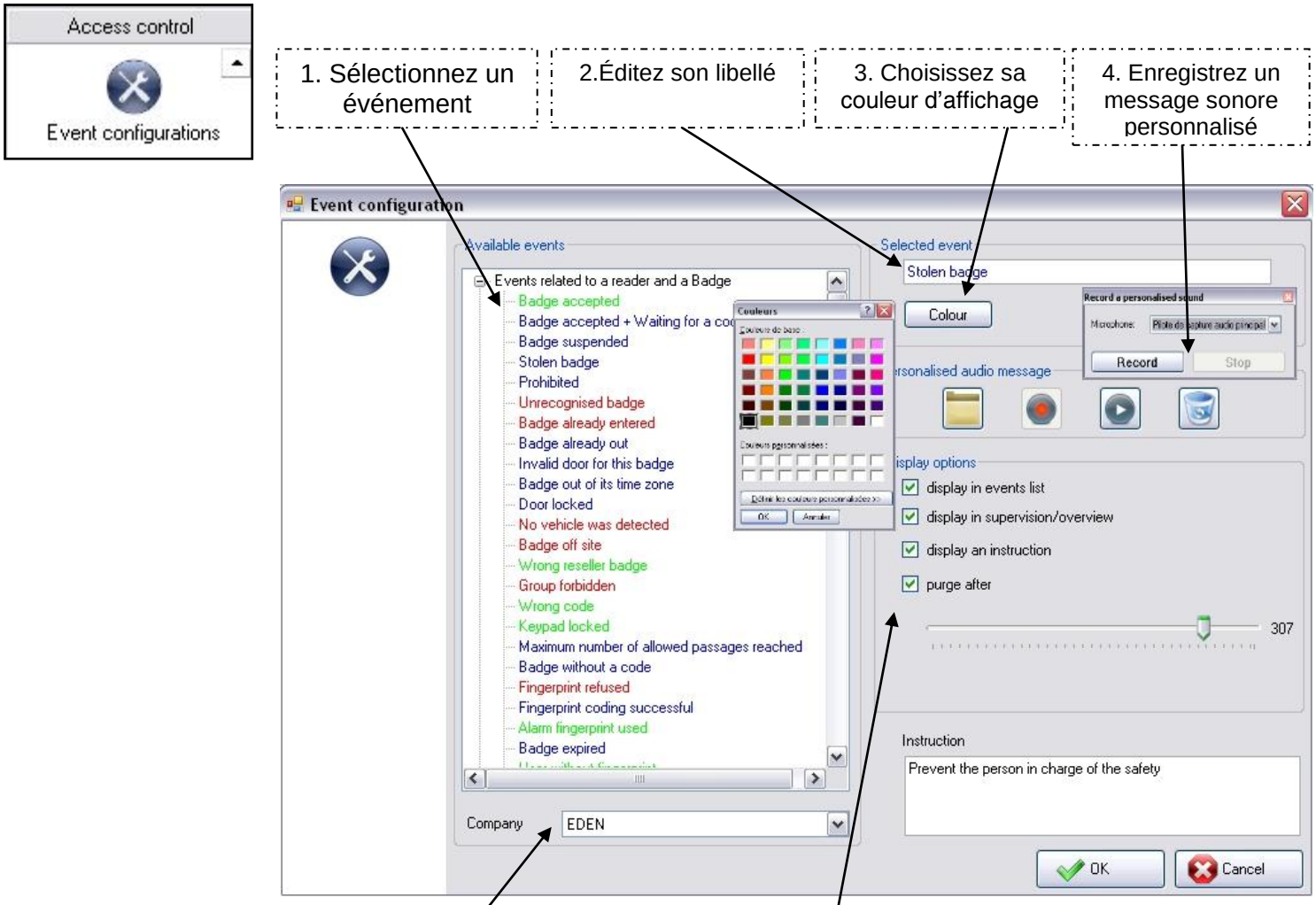
Les applications « logiciel »

Liste des événements

Sélectionnez Contrôle d'accès → Paramétrage des événements

1. Paramétrage des événements

Ce menu permet de paramétrer les événements générés par la gestion des accès et des alarmes Intrusion du site. Chaque événement peut être filtré, généré un son et d'afficher sous une couleur préétablie.
une fois paramétrés, ces événements s'afficheront dans la liste des événements (voir page 132).



Gestion multi-locataires/sociétés

Réitérez cette procédure pour chaque locataire ou société

Paramétrez les options d'affichage

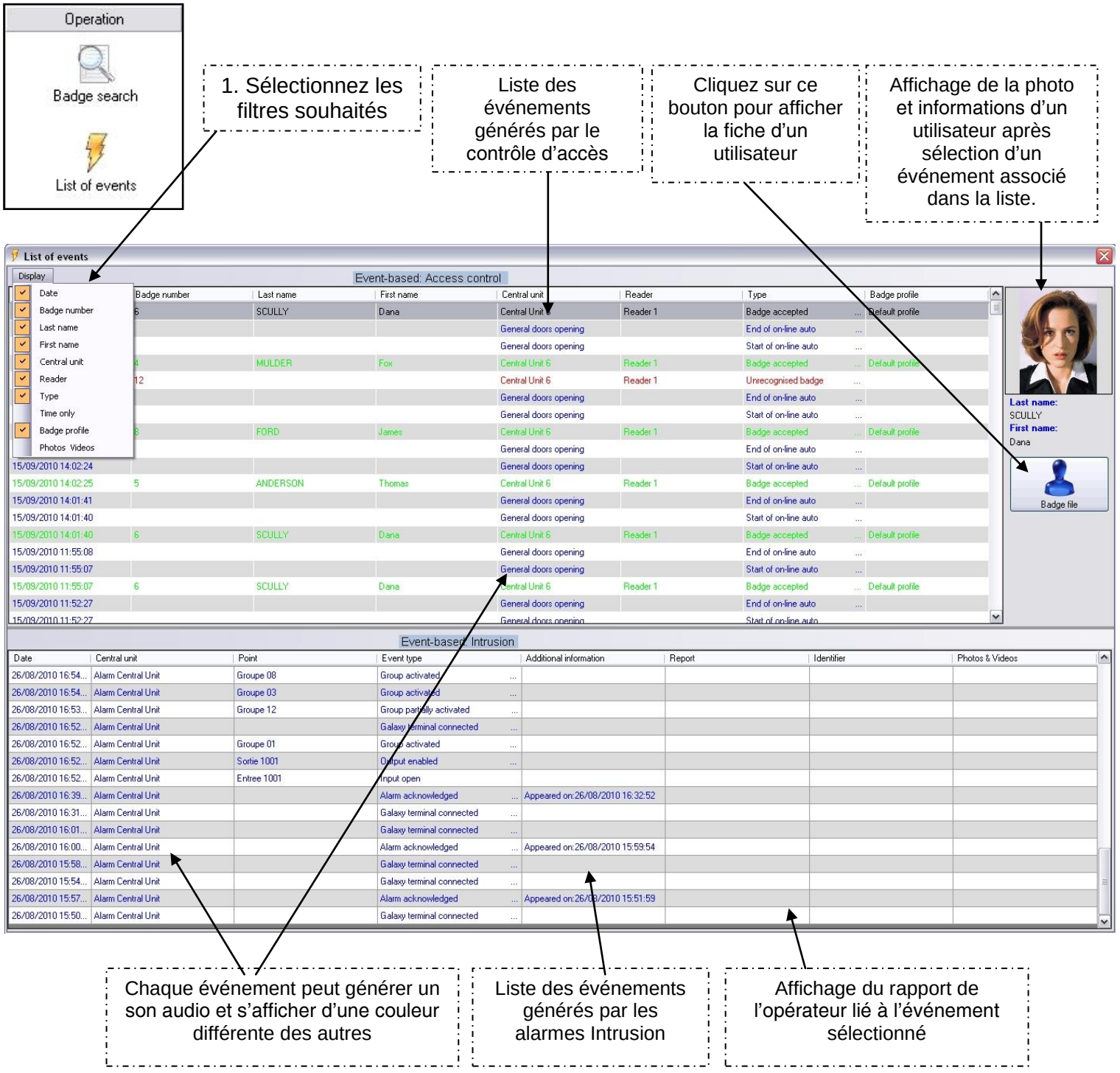
- Afficher ou pas l'événement dans la liste des événements
- Afficher ou pas dans la Supervision
- Afficher ou pas une consigne (Éditez la consigne si besoin)
- Purger ou pas l'événement suivant une durée paramétrée

Les applications « logiciel »

Liste des événements

2. Journal fil de l'eau

Cette application permet d'afficher la liste des événements générées pas le contrôle d'accès et les alarmes intrusion si le module optionnel correspondant est activé.



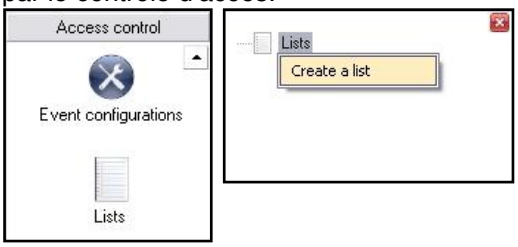
Les applications

Liste des événements

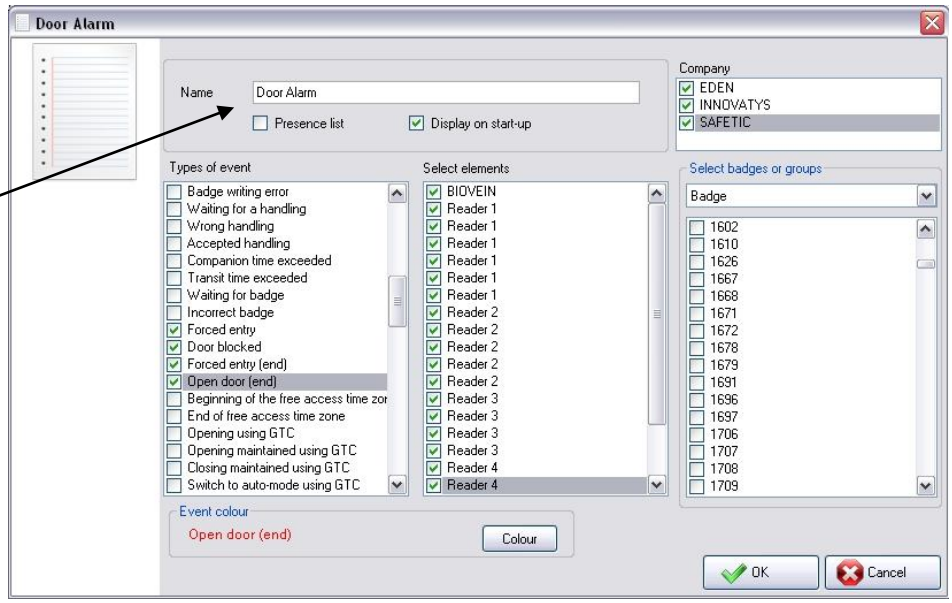
Sélectionnez l'onglet « Contrôle d'accès » → Listes

3. Les listes

Cette application permet de créer plusieurs listes d'événement « fil de l'eau » paramétrables pour les événements générés par le contrôle d'accès.



Cliquez sur « Listes »

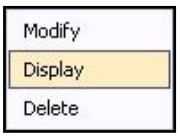


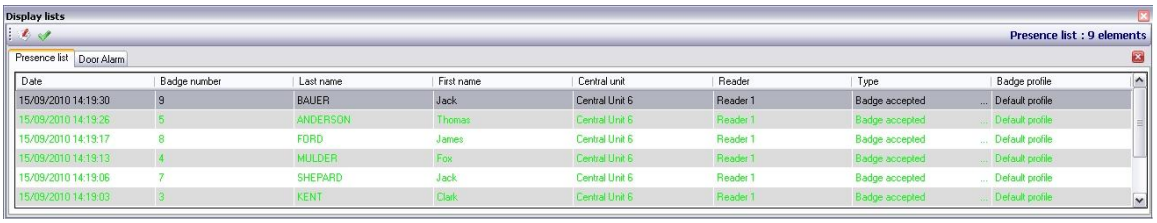
Procédure

1.Éditez le libellé de la liste,
2. Cochez la case « Afficher au démarrage » si besoin,
3. Sélectionnez le type de liste,

- Liste des présents
- Liste fil de l'eau

4. Si choix « B », sélectionnez dans le menu déroulant « type d »événements » les événements souhaités,
5.Éditez une couleur pour chaque événement,
6. Sélectionnez les lecteurs ou seront générés les événements sélectionnés,
7. Si certains événements sélectionnés sont associés à des badges/groupes d'accès, un filtre supplémentaire est disponible par badge ou par groupe d'accès,
8. Sélectionnez et cochez les locataires/sociétés associés à la liste si nécessaire




Display lists
Presence list : 9 elements
Presence list
Door Alarm
Date
Badge number
Last name
First name
Central unit
Reader
Type
Badge profile
15/09/2010 14:19:30 9 BAUER Jack Central Unit 6 Reader 1 Badge accepted Default profile
15/09/2010 14:19:26 5 ANDERSON Thomas Central Unit 6 Reader 1 Badge accepted Default profile
15/09/2010 14:19:17 8 FORD James Central Unit 6 Reader 1 Badge accepted Default profile
15/09/2010 14:19:13 4 MULDER Fox Central Unit 6 Reader 1 Badge accepted Default profile
15/09/2010 14:19:06 7 SHEPARD Jack Central Unit 6 Reader 1 Badge accepted Default profile
15/09/2010 14:19:03 3 KENT Clark Central Unit 6 Reader 1 Badge accepted Default profile

Il n'y a pas de limite du nombre de liste dans le logiciel.
Vous pouvez modifier ou supprimer une liste en la sélectionnant puis effectuez un clic droit ou gauche.
La case « Afficher au démarrage », permet d'afficher les listes automatiquement au démarrage du logiciel, sans avoir à le faire manuellement.
La fenêtre des listes apparaît en bas du logiciel. Vous pouvez à tout moment fermer une liste ou l'application totale.Tous les événements affichés dans ces listes sont enregistrés dans la base de données du serveur du logiciel et peuvent générer des rapports « historique ».

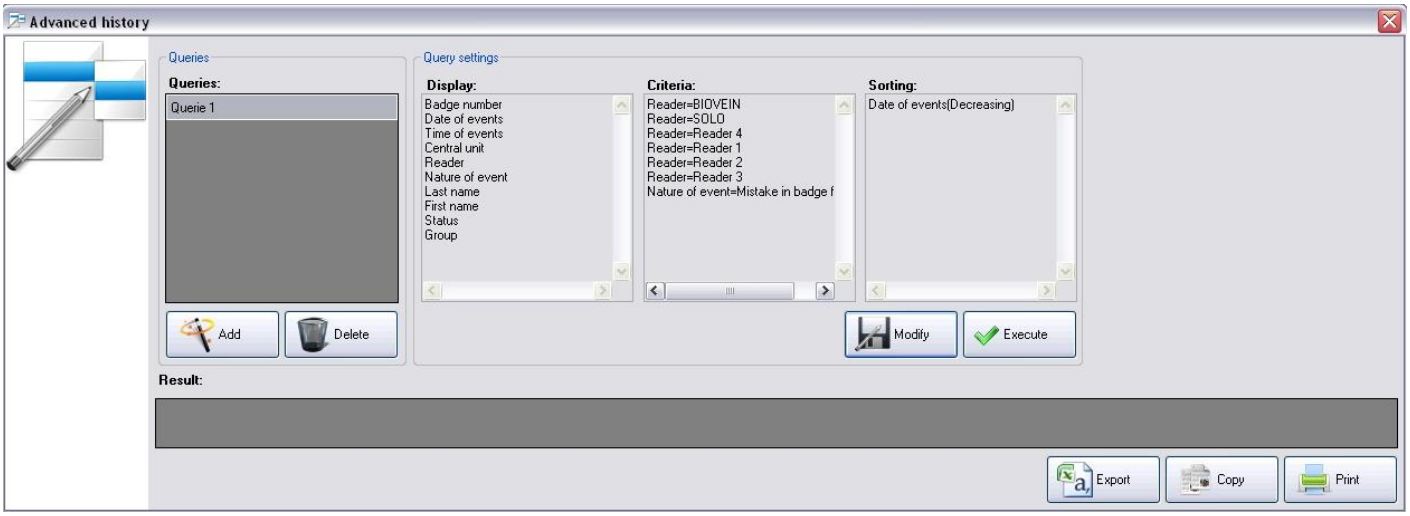
Les applications « logiciel »

Historique avancé

Sélectionnez l'onglet Exploitation

L'historique avancé est un outil permettant des requêtes afin d'obtenir des informations sur les badges et/ou les évènements liés à ces badges.
L'historique avancé dispose d'un assistant de création de requêtes destinées à simplifier la création de celles-ci. Cette application permet aussi l'exportation des résultats des requêtes vers un format CSV pour les tableurs, ou de copier le tableau résultat dans le presse-papier ou encore de l'imprimer.

- Cliquez sur « Historique avancé »



Détail des différentes options disponibles

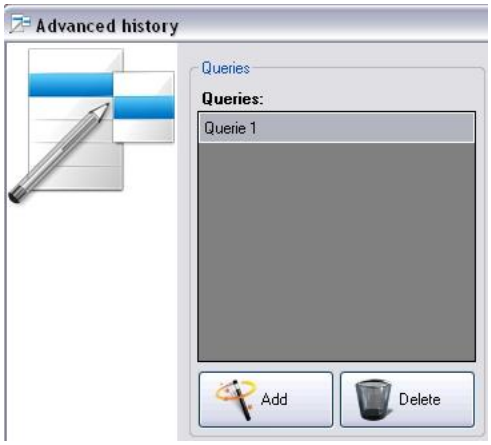
« Requêtes »
Liste des requêtes préétablies.
« Ajouter »
Ajoute une requête en lançant l'assistant.
« Supprimer »
Supprime la requête sélectionnée.
« Modifier »
Modifie la requête sélectionnée via l'assistant.
« Exécuter »
Exécute la requête sélectionnée et affiche le résultat dans le tableau "Résultat".
« Exporter »
Exporte le tableau résultat actuellement affiché vers un fichier au format CSV.
« Copier »
Copie le tableau résultat actuellement affiché dans le presse papier.
« Imprimer »
Imprime le tableau résultat actuellement affiché.

Les applications « logiciel »

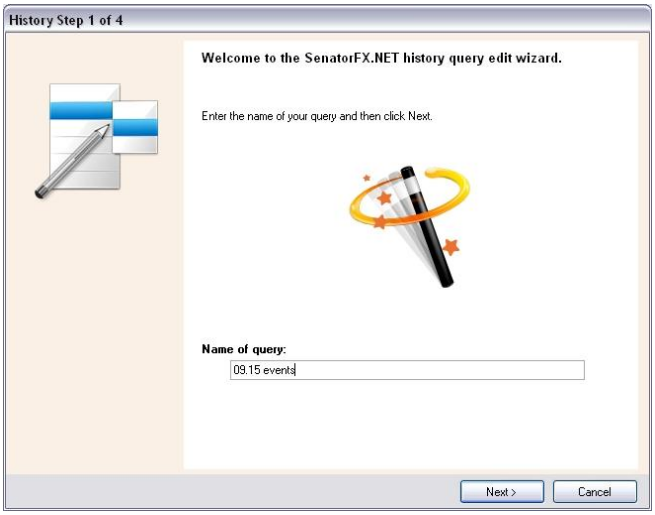
Historique avancé

Sélectionnez l'onglet Exploitation

Cliquez sur « Historique avancé »
Puis cliquez sur le bouton
« Ajouter »
Créez votre requête en 4 étapes

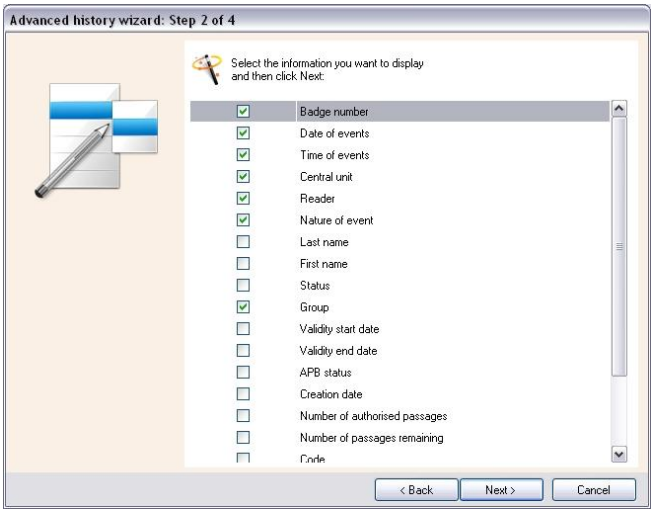


Étape 1 sur 4


History Step 1 of 4
Welcome to the SenatorFX.NET history query edit wizard.
Enter the name of your query and then click Next.
Name of query:
09.15 events
Next >
Cancel

-
Éditez le nom de la requête qui s'affichera dans l'application
-Cliquez sur le bouton « suivant »

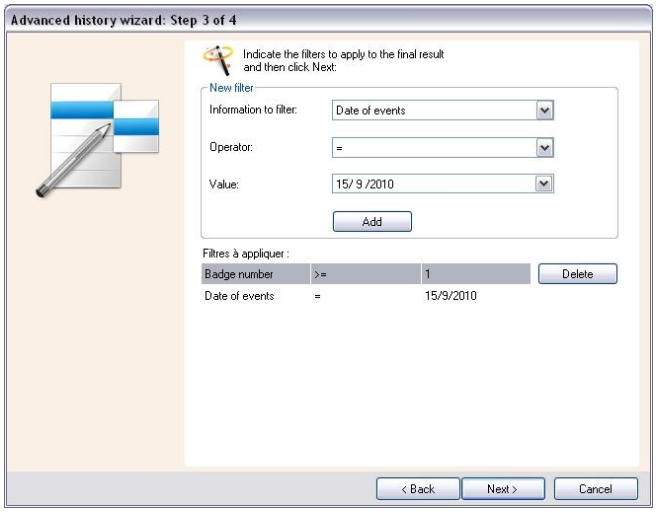
Étape 2 sur 4



-Sélectionnez et cochez les différentes informations que vous souhaitez afficher dans la requête
-Cliquez sur le bouton « suivant »

Étape 3 sur 4

-Entrez les critères de filtrage de votre requête
-Les filtres déjà définis sont listés en dessous de "Filtres à appliquer ».
-Vous pouvez retirer des filtres en cliquant sur "Supprimer".

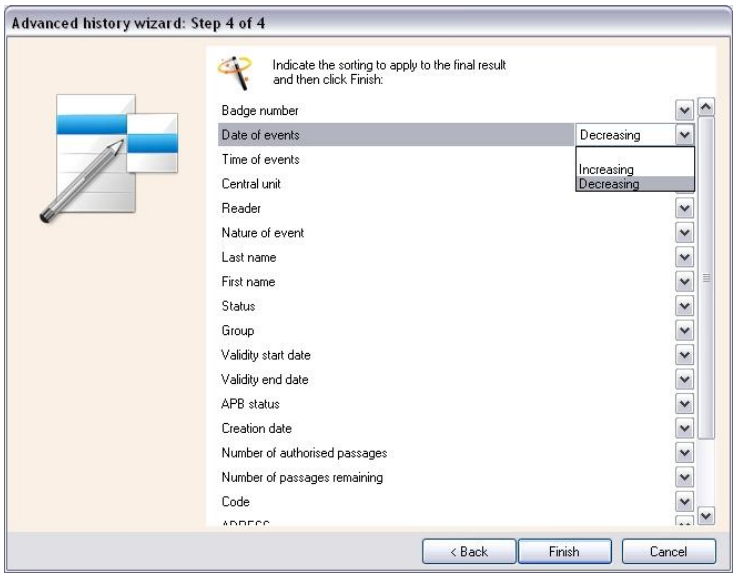


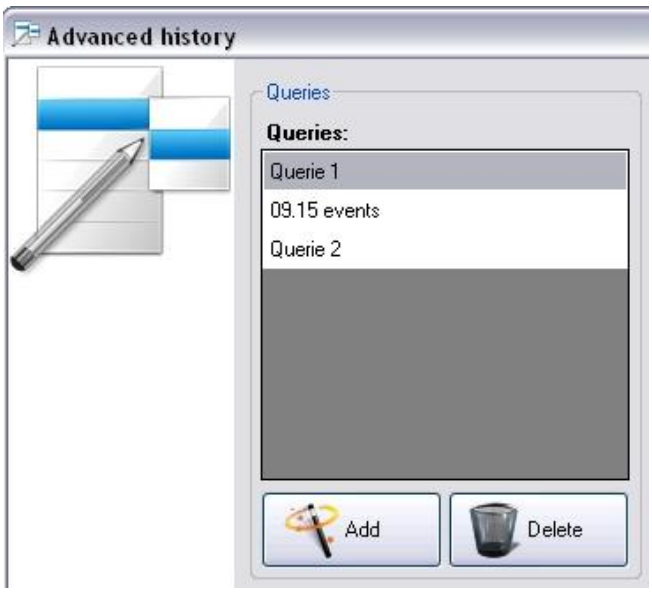
Les applications

Créez votre requête en 4 étapes (suite)

Étape 4 sur 4

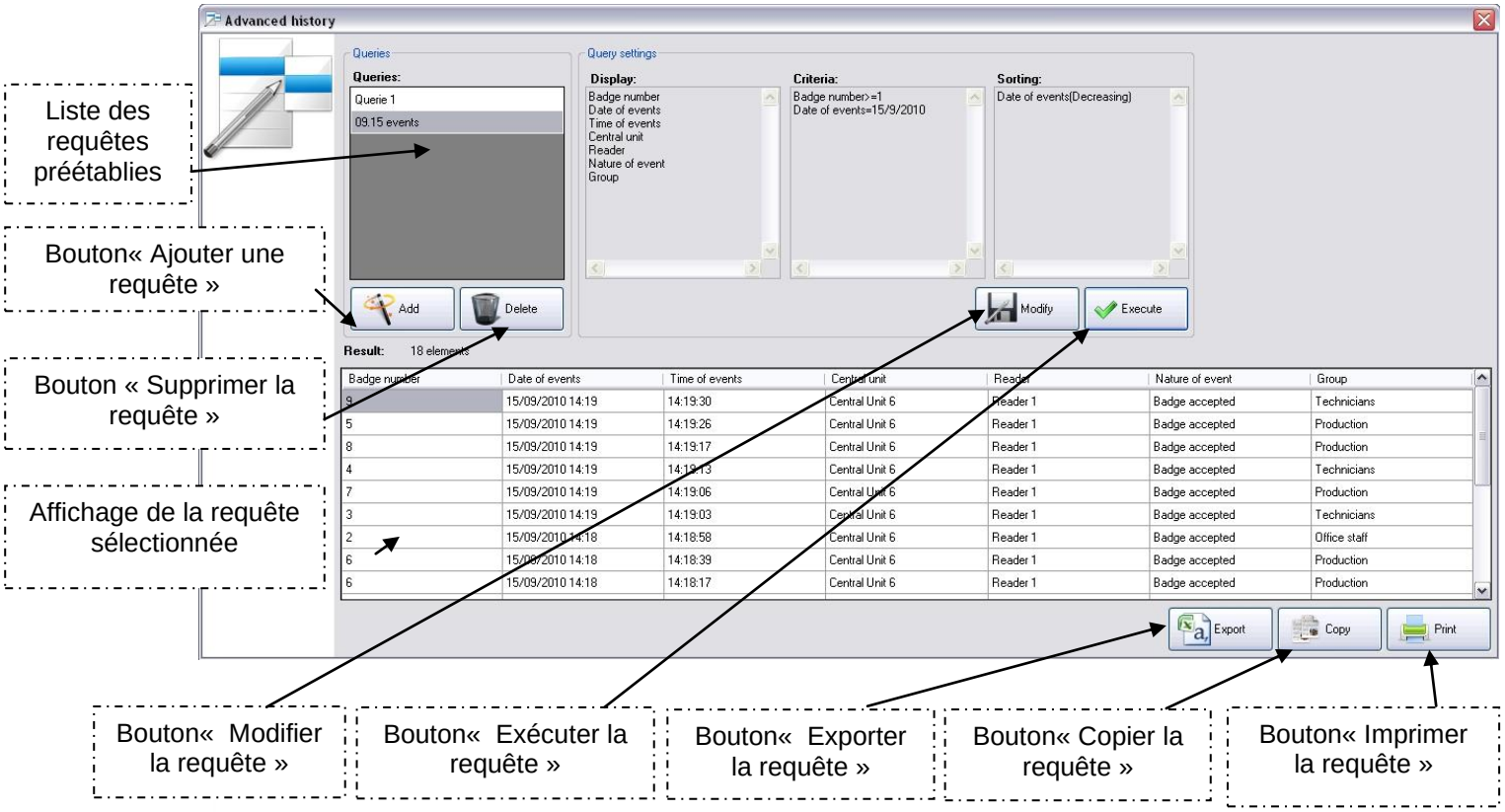
-Déterminez les tris à appliquer au résultat final
-Cliquez sur le bouton « Terminer »





La nouvelle requête apparait dans la liste

Vous pouvez exécuter la requête, puis l'imprimer ou l'exporter…


Advanced history
Queries
Queries:
Querie 1
09.15 events
Query settings
Display:
Badge number
Date of events
Time of events
Central unit
Reader
Nature of event
Group
Criteria:
Badge number>=1
Date of events=15/9/2010
Sorting:
Date of events(Decreasing)
Add
Delete
Modify
Execute
Result: 18 elements
Badge number | Date of events | Time of events | Central unit | Reader | Nature of event | Group
9 | 15/09/2010 14:19 | 14:19:30 | Central Unit 6 | Reader 1 | Badge accepted | Technicians
5 | 15/09/2010 14:19 | 14:19:26 | Central Unit 6 | Reader 1 | Badge accepted | Production
8 | 15/09/2010 14:19 | 14:19:17 | Central Unit 6 | Reader 1 | Badge accepted | Production
4 | 15/09/2010 14:19 | 14:19:13 | Central Unit 6 | Reader 1 | Badge accepted | Technicians
7 | 15/09/2010 14:19 | 14:19:06 | Central Unit 6 | Reader 1 | Badge accepted | Production
3 | 15/09/2010 14:19 | 14:19:03 | Central Unit 6 | Reader 1 | Badge accepted | Technicians
2 | 15/09/2010 14:18 | 14:18:58 | Central Unit 6 | Reader 1 | Badge accepted | Office staff
6 | 15/09/2010 14:18 | 14:18:39 | Central Unit 6 | Reader 1 | Badge accepted | Production
6 | 15/09/2010 14:18 | 14:18:17 | Central Unit 6 | Reader 1 | Badge accepted | Production
Export
Copy
Print
Liste des requêtes préétablies
Bouton« Ajouter une requête »
Bouton « Supprimer la requête »
Affichage de la requête sélectionnée
Bouton« Modifier la requête »
Bouton« Exécuter la requête »
Bouton« Exporter la requête »
Bouton« Copier la requête »
Bouton« Imprimer la requête »

Assistance technique

Notre assistance technique est réservée uniquement aux professionnels de la sécurité.

Notre support technique est disponible du lundi au vendredi de 9h à 12h et de 14h à 18h (17h le vendredi)

hotline@eden-innovations.com

Nous assurons des formations techniques quant à l'utilisation des produits conçus par EDEN INNOVATIONS.

Toutes nos formations sont effectuées dans les locaux de la société EDEN INNOVATIONS.

Si vous êtes un utilisateur à la recherche

- D'informations sur l'utilisation de notre solution
- D'un professionnel de la sécurité pour la maintenance de votre site
- De conseils pour l'élaboration d'un cahier des charges particulier

Contactez notre standard

04 42 24 70 40

Zone Commerciale et Artisanale
670, route de Berre
13510 EGUILLES
France

www.eden-innovations.com